ISMS 適合性評価制度に関する
アンケート調査報告書

2014 年 10 月

一般財団法人 日本情報経済社会推進協会（JIPDEC）
情報マネジメント推進センター

目　　次

はじめに

このたびは、ご多忙の中、ISMS 適合性評価制度に関するアンケート調査にご協力を賜り、厚く御礼申しあげます。おかげさまで、多数の組織様から、貴重なデータとともに、数多くの有益なご意見、ご要望等を頂戴することができました。調査結果につきましては、本書で概要をご報告するとともに、今後の制度の運営に積極的に活用させていただく所存です。

ISMS 適合性評価制度は、民間主体の制度として 2001 年度にスタートし、約 1 年間のパイロット運用を経て、2002 年 4 月から本格運用に入り、今日に至っております。

この間、コンピュータ処理への依存度の高まりやインターネットの爆発的な広がりとともに、それに比例して情報資産への脅威も増大し、システムや人的な脆弱性を突いたセキュリティ事故も件数、規模ともに増加してきています。このような背景から、自社のみならず取引先における情報セキュリティ管理のリスクを把握する重要性についての認識は格段に高まってまいりました。

これを受けて 2008 年及び 2011 年に、ISMS 制度の実態を把握し、制度の信頼性をより高めることを目的としてアンケートを実施しました。本調査は、前回調査から 2 年が経過し、新たに約 500 の組織が認証を取得されたことから、現時点での ISMS 適合性評価制度の状況を確認するとともに、ISMS 導入及び認証の有効性を検証し、制度の改善を図ることを目的としています。

本報告書で調査結果の概要をご報告するとともに、今後、調査結果に対して更に分析、検討を進め、皆様にとってなお一層有効で、活用度の高い制度にするために、必要な対応策を講じていく所存です。

また、関連機関、関係者がそれぞれの立場、視点で、調査結果を ISMS 制度の改善のためにご活用いただければ幸いです。

2014 年 10 月

一般財団法人 日本情報経済社会推進協会（JIPDEC）
情報マネジメント推進センター

調査の概要

調査内容
付録の「ISMS 適合性評価制度に関するアンケート調査書」を参照。
調査項目は以下のとおり。
・基本情報について
・ISMS 認証の運用実績等について
・ISMS の導入及び認証取得の効果等について
・審査員の力量及び審査の質について
・認証機関の認定の信頼性について
・制度全般に対するご意見等

調査対象
調査開始の 2014 年 3 月時点で、本協会が認定した ISMS 認証機関から ISMS 認証を取得した組織のうち登録情報を公開している 4,202 組織。

調査方法
郵送した調査書の質問（選択形式及び記述形式）に回答、返信していただく。

調査期間
2014 年 2 月下旬～3 月下旬。

有効回答数、回収率
有効回答数：　1,076 件
回収率：　25.6%

基本情報について

質問１　法人の業種

23 種類の業種区分について尋ねたところ、「情報技術」(64.6%)が突出しており、以下「その他サービス」(11.8%)、「建設業(エンジニアリングを含む)」(4.2%)、「出版･印刷業」(4.1%)が続いている（図 1-1)。

なお、この質問の集計結果は、同一法人の中の複数の部門が個別に認証を取得している場合、同一法人の情報を重複して集計したものであることに注意されたい。

業　種　区　分	組織	(%)	業　種　区　分	組織	(%)
1.　食料品･飲料･タバコ等の製造業	1	0.1	13.　建設業(エンジニアリングを含む)	45	4.2
2.　衣服･天然素材繊維製品の製造業	0	0.0	14.　廃棄物処理業･再生業	13	1.2
3.　木材･木製品･パルプ･紙等の製造業	3	0.3	15.　電力･ガス･熱･水道供給業	0	0.0
4.　出版･印刷業	44	4.1	16.　卸売･小売業	40	3.7
5.　化学薬品･化学製品(化学繊維を含む)･医薬品の製造業	2	0.2	17.　金融･保険･不動産業	14	1.3
6.　石油･石炭･ゴム･プラスチック等の製造業	0	0.0	18.　情報技術	690	64.6
7.　ガラス･セラミック･コンクリートの製造業	0	0.0	19.　ホテル･レストラン業	0	0.0
8.　鉄鋼･非鉄金属業･金属製品の製造業	2	0.2	20.　医療関係	7	0.7
9.　機械･機器の製造業	11	1.0	21.　その他サービス業	126	11.8
10.　電気/電子機器･光学的装置製造業	34	3.2	22.　公共･行政･教育機関	13	1.2
11.　輸送機器製造業	4	0.4	23.　分類不明	16	1.5
12.　その他の製造業	3	0.3%	合計	1,068	

（回答なし:8）

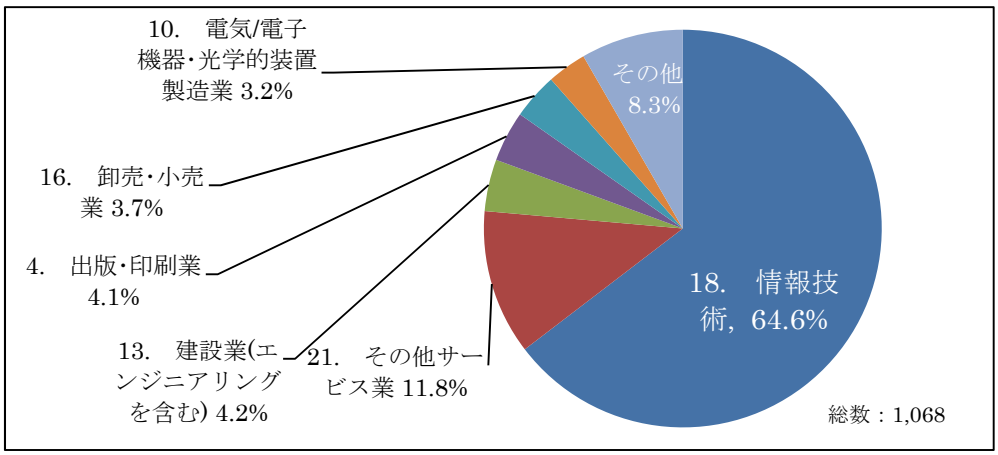


図 1-1　法人の業種

「情報技術」の内訳として 11 件の小区分を尋ねたところ、「受注ソフトウェア業」(33.2%)、「システムインテグレーション業」(28.1%)で過半数を占め、以下「ソフトウェアプロダクト業」(7.0%)、「計算事務等情報処理業」(5.2%)の順となっている（図 1-2)。

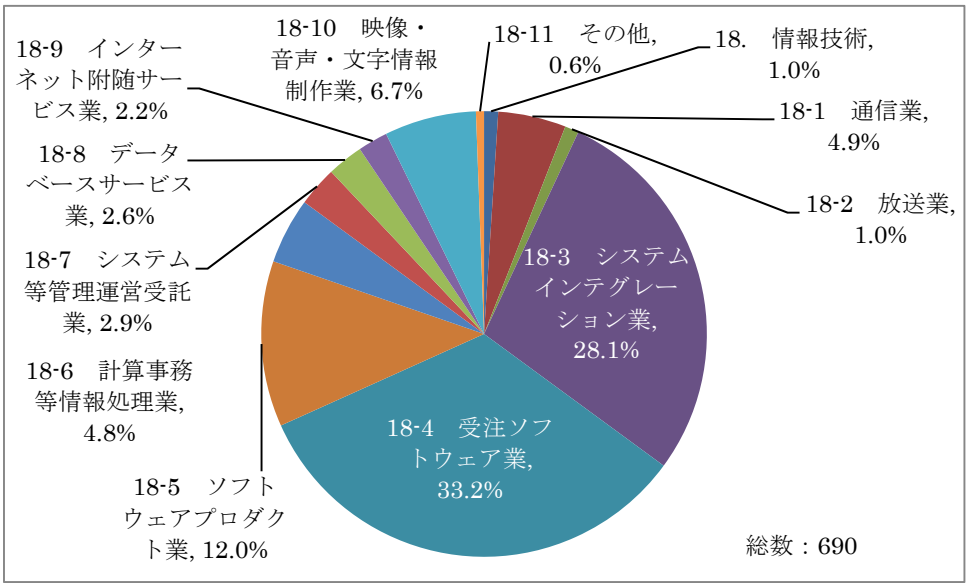


図 1-2　情報技術の内訳

質問２　資本金

法人が株式会社の場合、資本金を尋ねたところ、「5000 万円以下」(47.0%)が最も多く、対極の「3 億円超」(25.9%)　で続き、以下「5000 万円超、1 億円以下」(18.3%)、「1 億円超、3 億円以下」(8.8%)となっている（図 2)。

なお、この質問の集計結果は、同一法人の中の複数の部門が個別に認証を取得している場合、同一法人の情報を重複して集計したものであることに注意されたい。

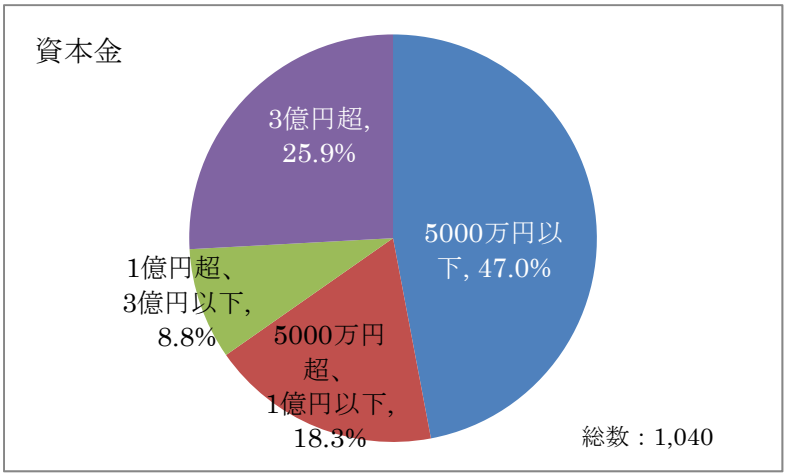


図 2　資本金

質問３　従業員数

法人が常時使用する従業員の数については、「300 人超」(29.8%)が最も多く、「100 人超、300 人以下」(25.2%)、「50 人超、100 人以下」(17.9%)の順となっている（図 3)。

なお、この質問の集計結果は、同一法人の中の複数の部門が個別に認証を取得している場合、同一法人の情報を重複して集計したものであることに注意されたい。

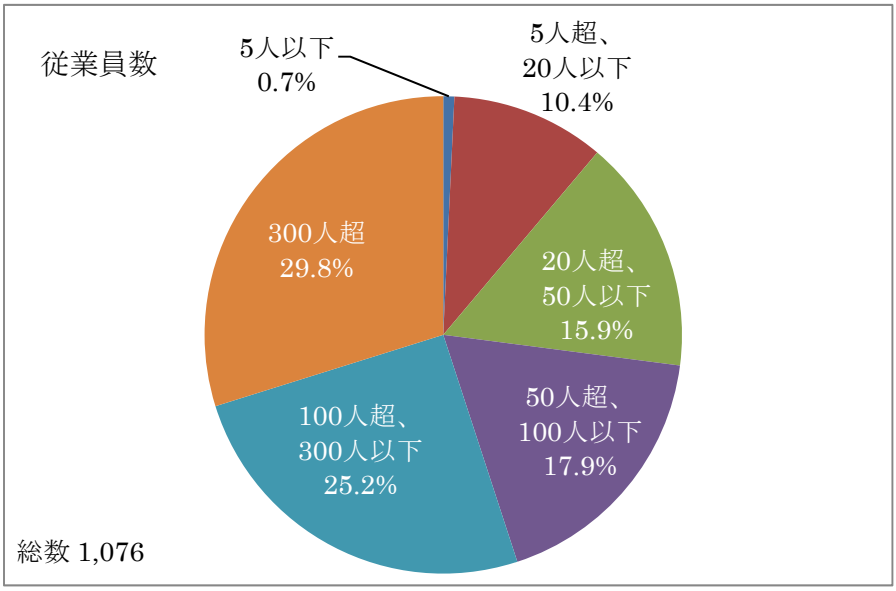


図 3　従業員数

質問４　ISMS 取得の認証範囲について

認証範囲の従業員数について、全社からみた割合について尋ねた結果を分類したところ、下記の表に示す結果が得られた。

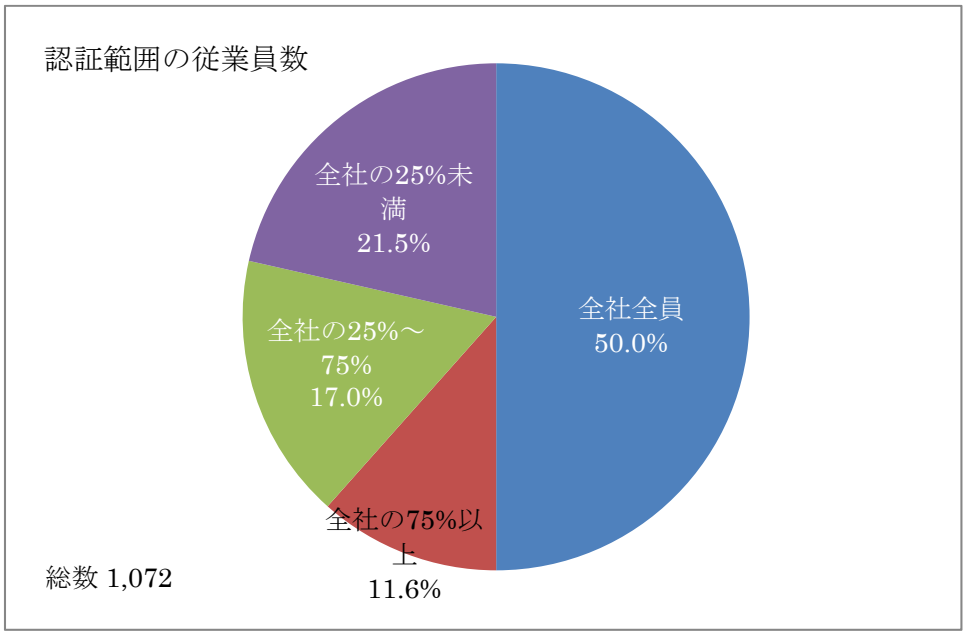


図４　認証範囲（従業員数の割合による）

有効回答数＝1,072	件数	割合（%）
全社	536	50.0
全社の 75%以上	124	11.6
全社の 25%～75%	182	17.0
全社の 25%未満	230	21.5

また、認証範囲の従業員数についてその概数を尋ねたところ、「20 人超、100 人以下」(43.3%)、「100 人超、1,000 人以下」(31.4%)、「20 人以下」(21.7%)、「1,000 人超」(3.6%)の順となった。

「認証範囲に特筆すべき特徴があれば記入してください」との問いに関し、有効回答数 142 件のうち、「グループ企業による取得」との回答が 47 件（33.0%)、それ以外のほとんどが「一部認証」(88 件、(62.0%)) となっている。

ISMS 認証の運用実績等について

質問５　経過年数

ISMS 認証取得後の経過年数を年月数で尋ねた結果を、「１年以下」、「１年超３年以下」、「３年超５年以下」、「５年超」の４階級に分類して度数を調べた。その結果、「５年超」（52.8%）、「３年超５年以下」（19.9%）、「１年超３年以下」（16.9%）、「１年以下」（10.4%）の順となった（図 5）。

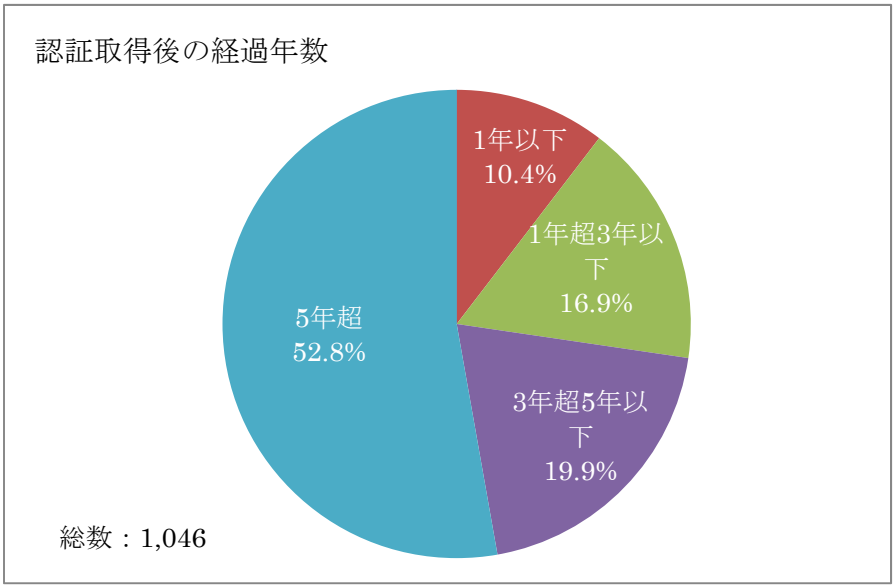


図５　経過年数

質問６　他のマネジメントシステム認証

ISMS 認証取得以外にどのようなマネジメント認証取得をしているかを尋ねた結果を、「ISO9001（品質）」、「ISO14001（環境）」、「ISO/IEC 20000（IT サービス）」、「ISO22301（事業継続）」、「その他」に分類して度数を調べた。その結果、

「ISO9001（品質）」（40.4%）、「ISO14001（環境）」(30.3%)、「ISO/IEC 20000（IT サービス）」(4.7%)、「ISO22301（事業継続）」（1.3%）の順となった。また、「その他」の 76.1%が、JIS Q 15001:2006(プライバシーマーク)であった（図 6)。

なお、この質問の集計結果は、同一法人が取得している他のマネジメントシステム認証を重複して集計したものであることに注意すること。

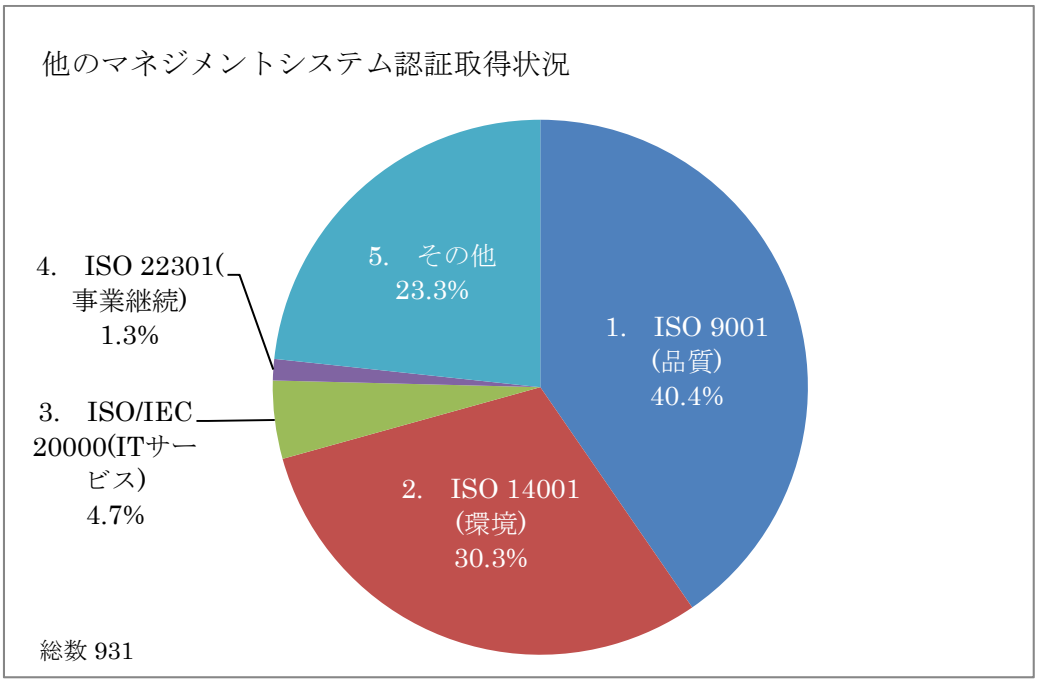


図 6　他のマネジメントシステム認証

質問７　認証機関の変更

ISMS 認証取得後から現在に至るまでに、認証機関（審査機関）を変更した、または検討したことを尋ねた結果を、「変更を考えたことはない」、「変更を考えたが、実行していない」、「1 回変更した」、「2 回以上変更した」に分類して度数を調べた。その結果、「変更を考えたことはない」（72.8%）、「変更を考えたが、実行していない」（15.9%）、「1 回変更した」（10.6%）、「2 回以上変更した」（0.7%）の順となった（図 7）。

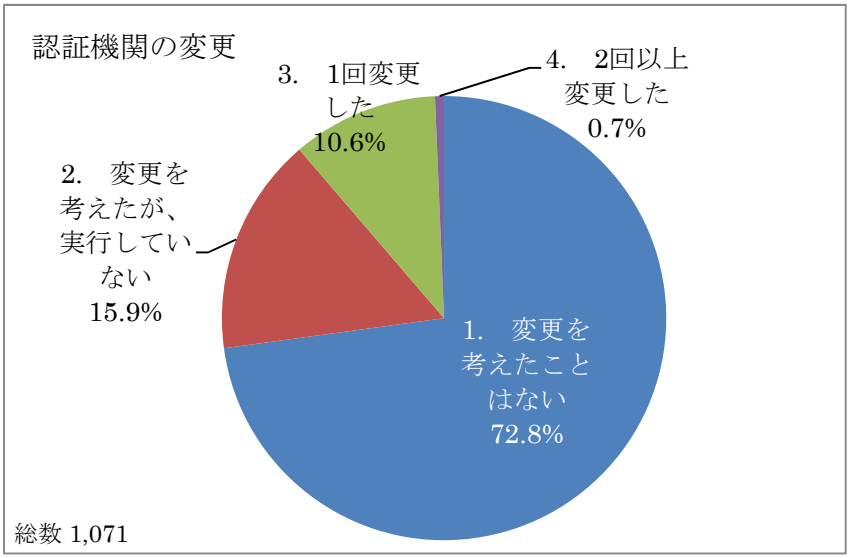


図 7　認証機関の変更

また、上記で「変更を考えたが、実行していない」、「1 回変更した」、「2 回以上変更した」と回答した 281 組織に対して、その理由として最もあてはまるものを回答してもらった結果、以下のように、「審査料金の比較」とした組織が 73%を占めた。

有効回答数＝281	件数	割合（%）
審査内容（深さや指摘内容等）が不満	19	6.8
認証機関のサービス（情報提供等）や対応（手続き等）に不満	15	5.3
審査料金の比較	205	73.0
その他	42	14.9

ISMS の導入及び認証取得の効果等について

質問８　導入の目的又は動機

ISMS 導入の目的又は動機について、９つの項目に「該当する」「やや該当する」「余り該当しない」「該当しない」の４段階で尋ねた結果は図８のとおりとなった。

全項目のうち、「該当する」の回答が最も多いものは「5. 顧客からの信頼を確保するため」(80.8%)、僅差で「2. 組織の情報セキュリティ対策の強化のため　」(79.6%)、「1 組織の情報セキュリティ管理体制の強化のため」(78.2%)、「3. 社員の情報セキュリティに関する意識向上、教育啓発のため」(76.6%)が続く。一方、「該当する」の回答が最も少ないものは「4. 入札、受注の条件、取引先からの要請による」(49.1%)であった。

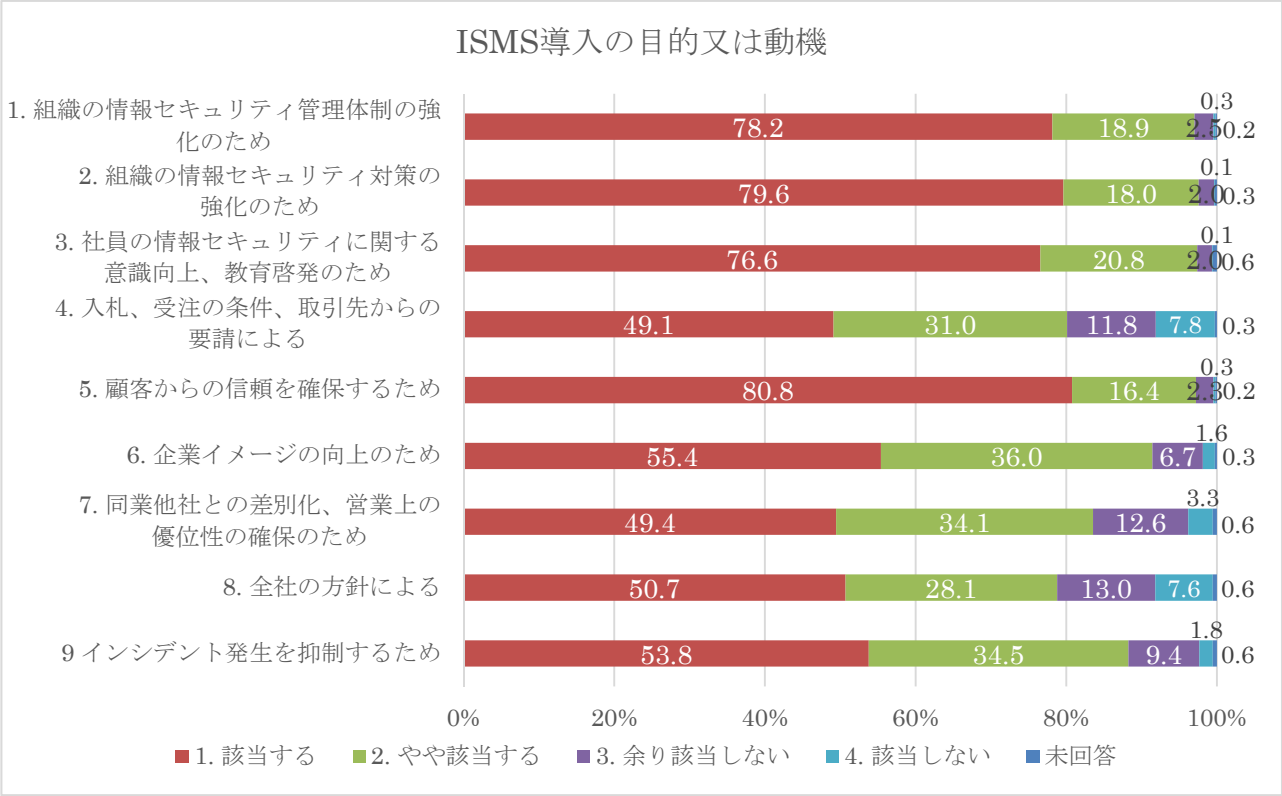


図８　導入の目的又は動機

項目 No.1 から項目 No.9 以外の導入の目的又は動機のうち、主な事項を以下に記す。

・お客様にご迷惑をかけないため
・安全に情報共有しながら情報活用したいため
・業務の効率化
・PDCA サイクルの考えを日常業務にも役立てる
・グループ会社の方針
・監督官庁の要請

質問９　ISMS 導入の効果

ISMS 導入の効果について、16 の項目に「該当する」「やや該当する」「余り該当しない」「該当しない」の４段階で尋ねた結果は図 9 のとおりとなった。

全項目のうち、「該当する」の回答が最も多いものは「2. 組織の情報セキュリティ対策が強化できた」(71.9%)、僅差で「1. 組織の情報セキュリティ管理体制が強化できた」(71.2%)、「3. 社員の情報セキュリティに関する意識高揚、教育啓発に寄与した」（69.9%）が続き、次いで「4. 顧客からの信頼確保に貢献した」(54.6%)となった。

一方、「該当する」の回答が最も低いものは、「7. 事業の収益向上に貢献した」（9.7%）、「8. IT 統制、J-SOX 法対応に有効であった」（10.9%）となった

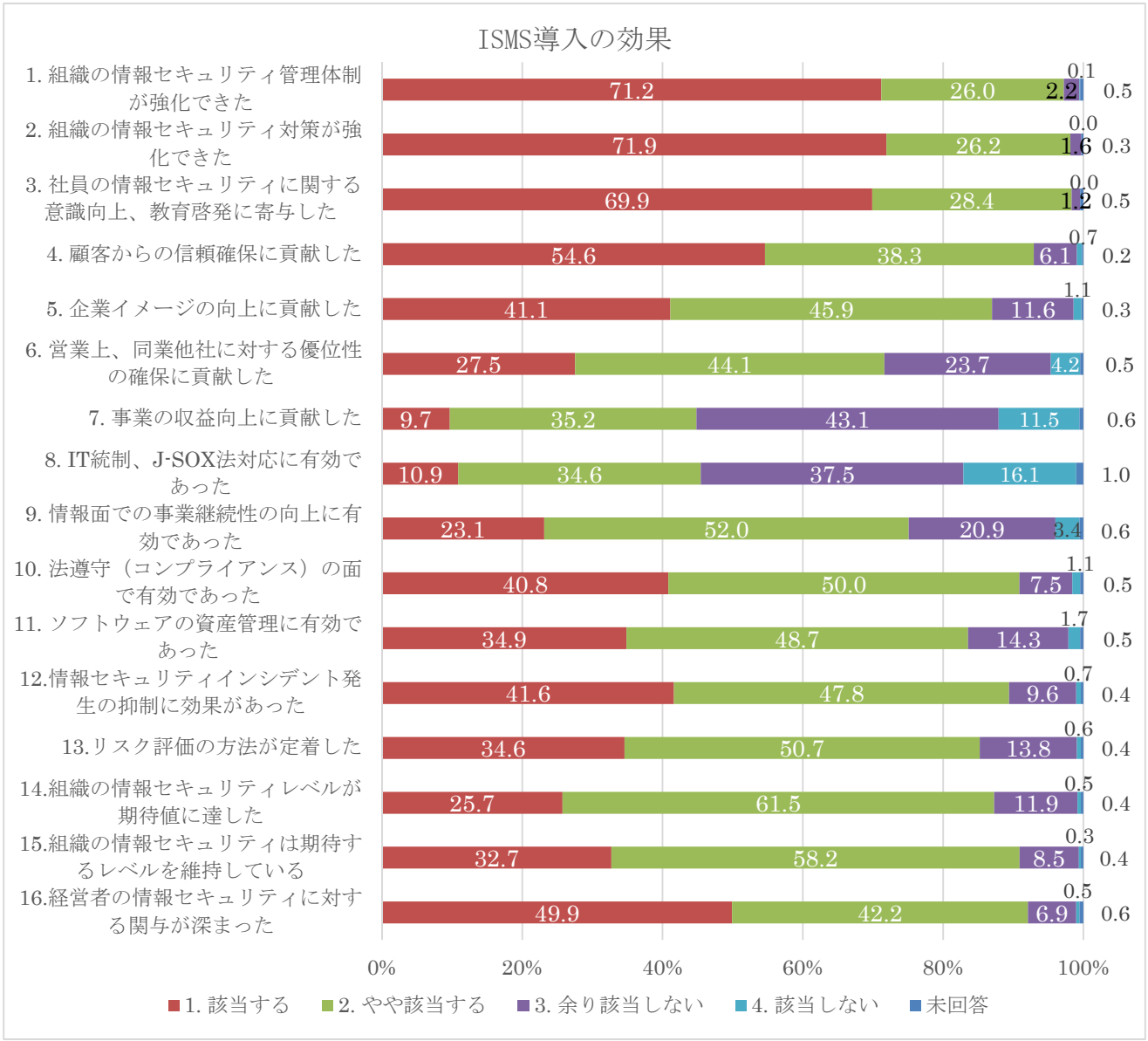


図 9　ISMS 導入の効果

項目 No.1 から項目 No.16 以外の導入の効果のうち、主な事項を以下に記す。

・リスクマネジメントの強化につながった

・収益向上に関してはあまり目に見える効果はないが、インシデント発生による収益低下のリスク回避には大きく貢献している

・事業継続の重要性が再認識できた

・業務遂行上における顧客との情報セキュリティ面での意識疎通がスムースになった

・海外組織との接触及び情報交換ができるようになった

・ISO 22301（事業継続マネジメントシステム）の認証取得がスムースに行えた

・全般的に証跡を残す習慣がついた

質問１０　顧客からの要求

顧客から、組織の情報管理リスクの把握のため、ISMS 認証文書（登録書）の他に要求されたことがあるかを尋ねたところ、図 10 に示す結果となった。

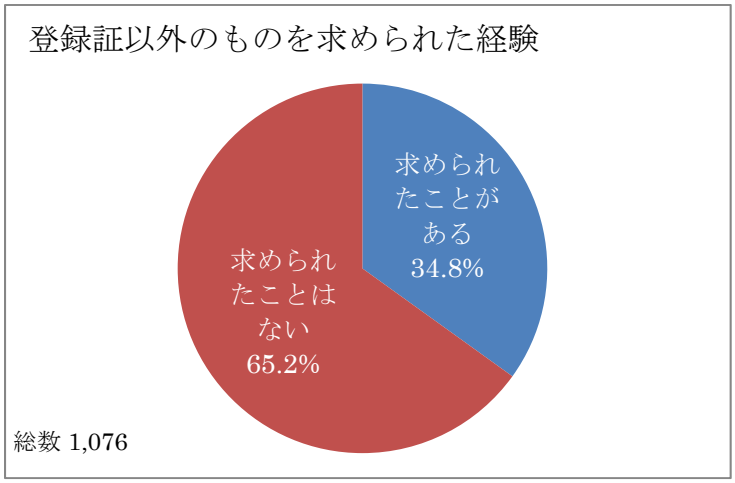


図 10　登録書以外に求められた経験

顧客から、組織の情報管理リスクの把握のため、要求された項目の代表的なものは以下のとおりとなった。

・実査、取引先よりのセキュリティ監査

・セキュリティ教育の有無

・アンケートへの回答

・情報セキュリティ自主チェックリストの提出

・社内のセキュリティルール、手順書などの提出

・機密情報に関する規定や記録など

・全搬統制、コンプライアンス遵守状況の提出

質問１１　ISMS に関する今後の課題

自組織の ISMS 認証取得、維持に関する今後の主な課題についての自由記述回答内容を分類した結果は図 11 のとおりである。

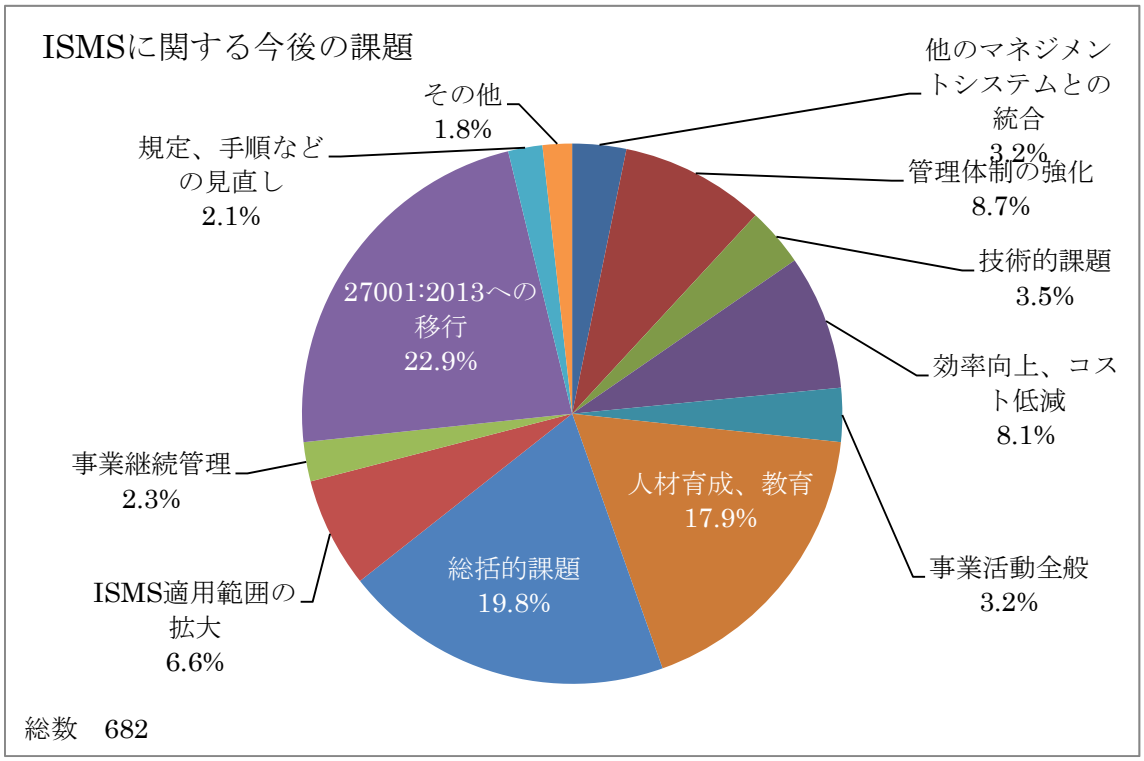


図 11　ISMS に関する今後の課題

・27001:2013 への移行：JIS Q 27001:2014 への移行
・総括的課題：マネジメントシステムの継続改善、形骸化の防止、運用の定着化など
・人材育成、教育：ISMS 推進要員の育成、社員の教育、意識高揚など
・ISMS 適用範囲の拡大：部門への適用から全社、グループ会社への適用拡大など
・効率向上、コスト低減：運用効率の向上、運用コスト低減、情報セキュリティと利便性のバランスなど
・管理体制の強化：ISMS の運用、管理体制の強化、リスクアセスメント・有効性評価などの強化
・技術的課題：新技術（クラウド、スマートフォンなど）への対応、ネットワーク監視などの管理策の強化、
・事業活動全般：経営、事業への反映、営業活動、顧客要求への対応、収益向上など
・他のマネジメントシステ証取得など
・事業継続管理：事業継続計画の策定、事業継続管理の推進
・規定、手順などの見直し
・その他

審査員の力量及び審査の質について

質問１２　審査員の力量

最近受審した審査での審査員の力量について、６つの項目に「十分である」「概ね十分である」「やや不十分である」「不十分である」の４段階で尋ねた結果は、図 12-1 のとおりとなった。

全項目のうち、「十分である」の回答が最も多いものは、「1 マネジメントシステムに関する知識及び業務経験」(74.3%)、次いで「2 情報システム、情報セキュリティに関する知識及び業務経験」(71.2%)、「4 コミュニケーション能力」(66.1%)、「5 審査技術」(65.4%)、「6 改善課題を指摘する能力」(62.6%)、「3 受審組織の業務に対する理解」(56.1%)の順となっている。

「十分である」及び「概ね十分である」の回答を加算したものの比率は、いずれの項目についても 95%を上回る高い値を示している。

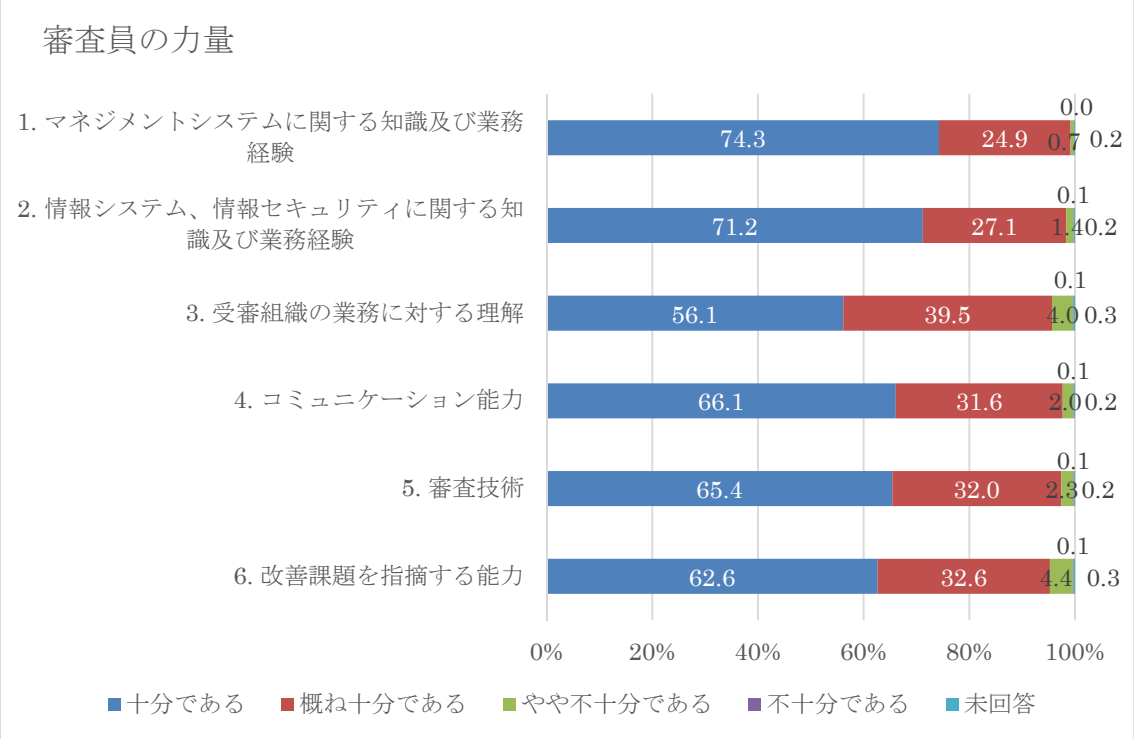


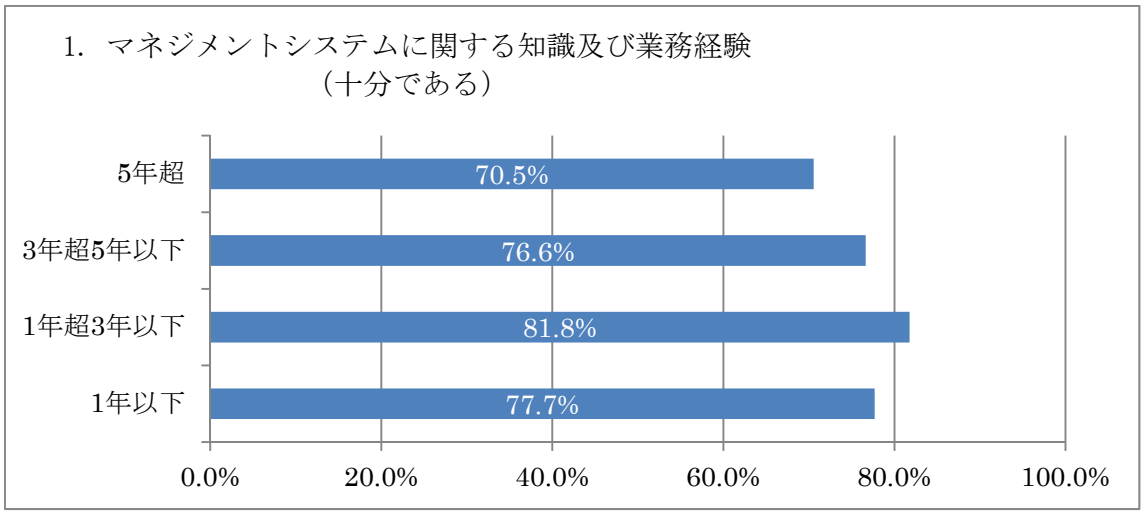
図 12-1　審査員の力量

質問１２と質問５とのクロス集計

審査員の力量に関する６つの項目の評価結果のうち、「十分である」の比率を、ISMS 認証取得後の経過年数の４階級ごとにクロス集計した結果を、図 12-2 に示す。

項目によって、若干の差異があるものの、ISMS 認証取得後の経過年数を経るにしたがって、「十分である」の比率が減少する傾向がみられる。特に、経過年数が３年を境にして、階段的に減少する傾向にある。

これは、受審側で ISMS の運用、改善の実績を積むに従い、審査に対する要求度、期待度が高くなるのは当然として、審査側の対応が受審側の要求、期待に応えきれていないことを示すものと思われる。特に、受審組織にとって ISMS 取得３年後に再認証審査を受けることが、審査に対する要求度が高まる契機になっているようである。



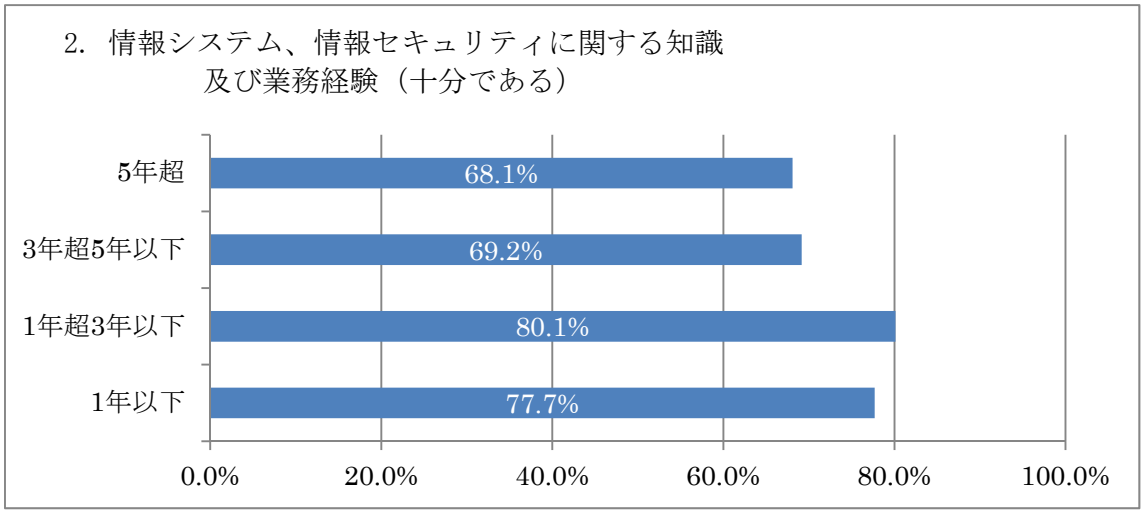
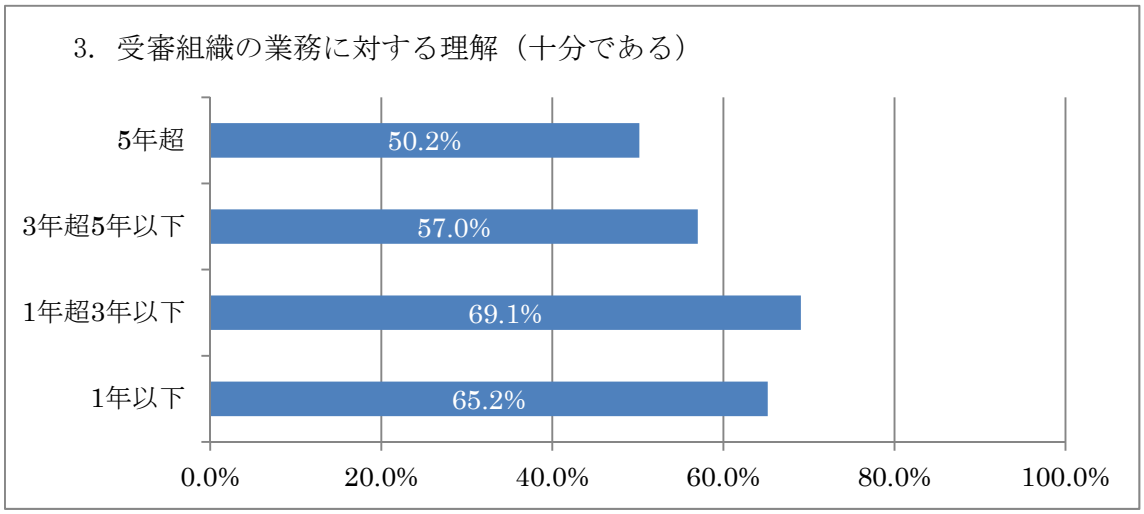
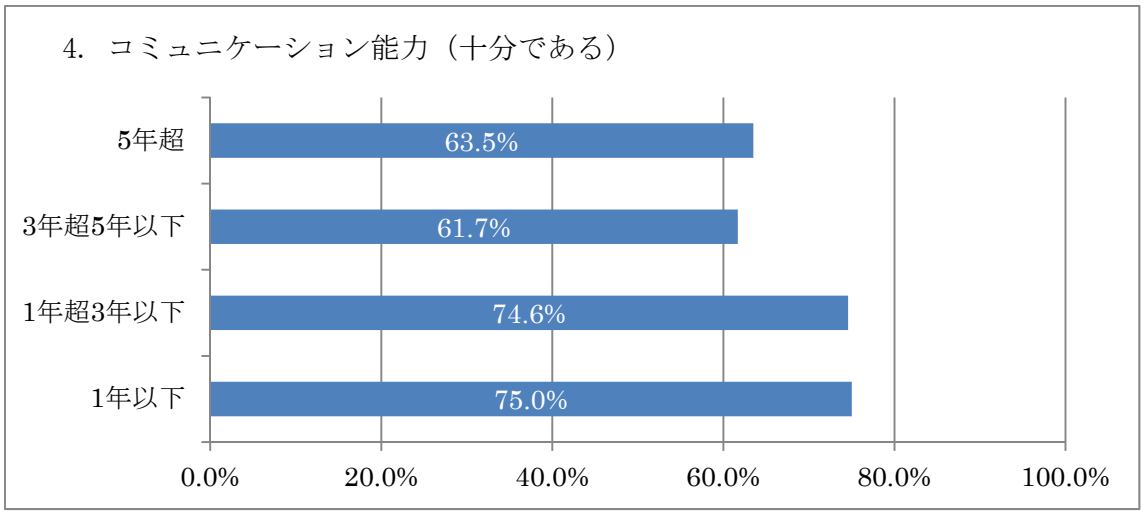


図 12-2　経過年数区分と審査員の力量(1/3)





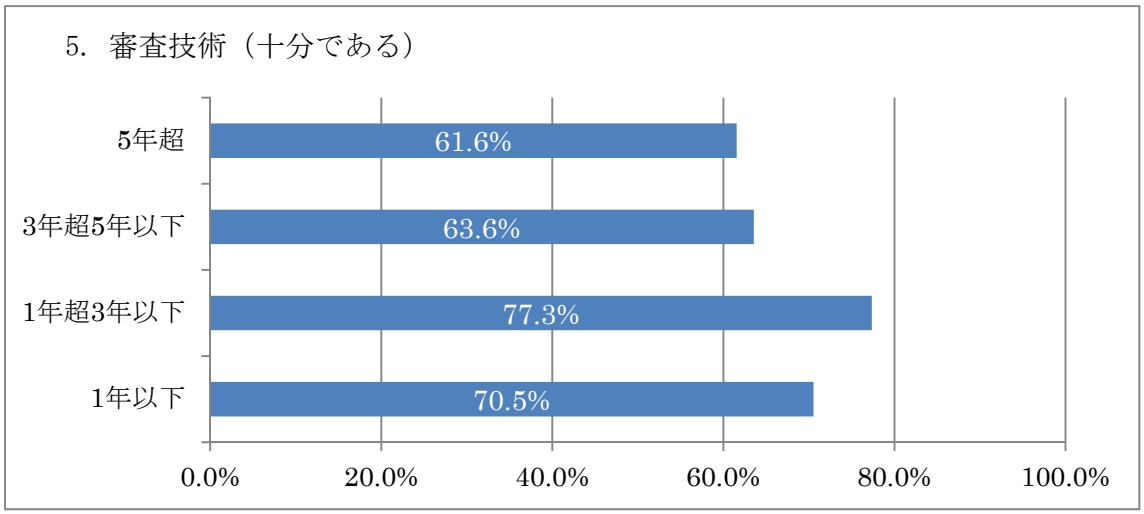


図 12-2　経過年数区分と審査員の力量(2/3)

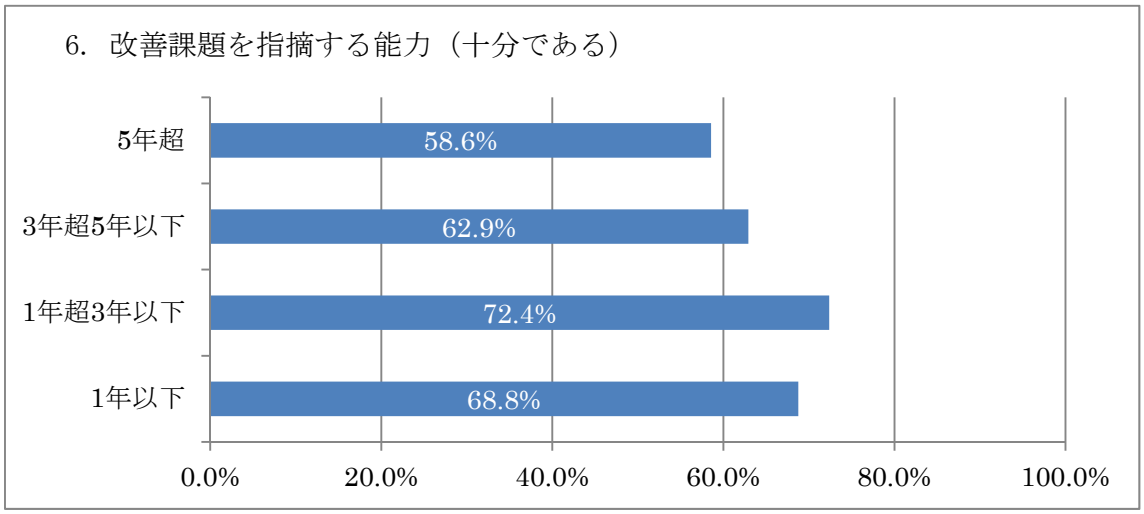


図 12-2　経過年数区分と審査員の力量(3/3)

質問１３　認証審査の質

最近受審した審査の質について、審査の内容、審査の時間、審査の所見・指摘、審査に対する総合評価の４つの観点で評価していただいた。

(1)審査の内容

審査の内容に関しては、規格適合性及び管理策の２つに分けて、「満足」「やや満足」「やや不満」「不満」の４段階で尋ねた。

(a)規格適合性に関する審査内容の評価は、「満足」(68.6%)、「やや満足」(29.3%)、「やや不満」(2.1%)、「不満」(0.0%)であった（図 13-1a)。

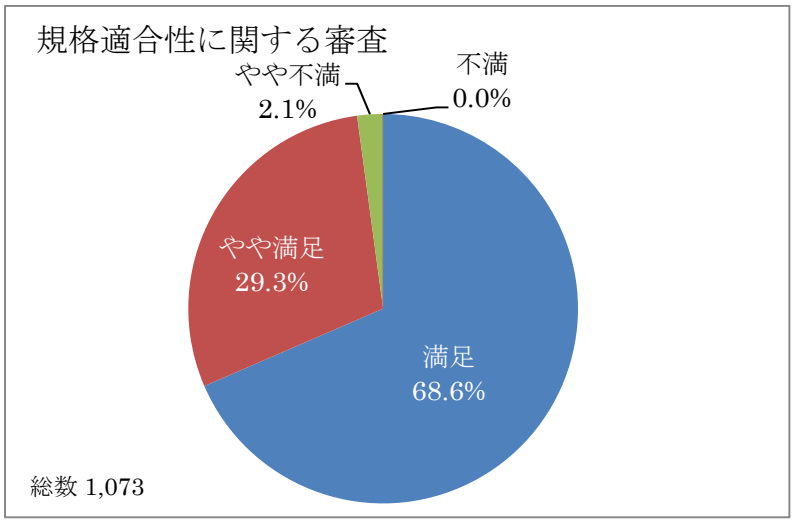


図 13-1a　審査の内容（規格適合性）

「やや不満」な点として指摘されたものの例は、次のとおり。

・前回審査との整合性がとれていない。
・観察事項（労働災害防止）は ISMS 外であり審査中に全く話がなかった。
・審査員によって規格の解釈が異なり、是正への指示が悩ましかった。
・スケジューリングにやや不満を感じた。審査が長時間すぎた。
・審査員の意見を押し付け気味だった。
・細かすぎる指摘が多い。

(b)管理策に関する審査内容の評価は、「満足」(62.4%)、「やや満足」(36.0%)、「やや不満」(1.5%)、「不満」(0.0%)の順であった（図 13-1b)。

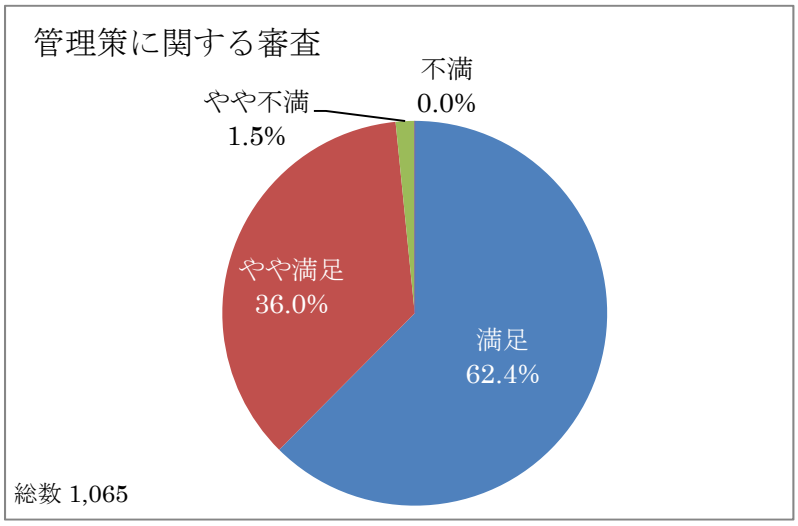


図 13-1b　審査の内容（管理策）

「やや不満」な点として指摘されたものの例は、次のとおり。

・自社の業務内容にフォーカスされていないように思えた。

・業務において対応が必須とされている管理策について審査員が理解していなかった。

・審査員の力量に差があると感じた。

・規格が要求していないことを要求する。・

(2)審査の時間

審査の時間の評価は、「適切」(77.4%)、「長い」(10.2%)、[何とも言えない」(9.6%)、「短い」(2.9%)の順であった（図 13-2）。

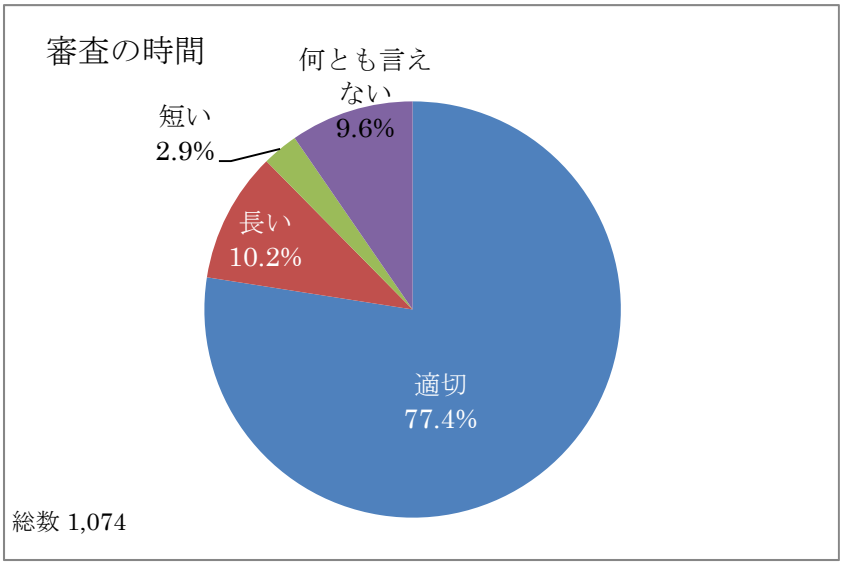


図 13-2　審査の時間

(3)審査の所見・指摘

審査の所見・指摘の有効性を、「大いに役立った」「役立った」「あまり役立たなかった」「役立たなかった」の４段階で尋ねた。

評価は、「役立った」(66.4%)、「大いに役立った」(31.5%)、「あまり役立たなかった」(2.0%)の順であった。「役立たなかった」の評価は 0.0%であった（図 13-3)。

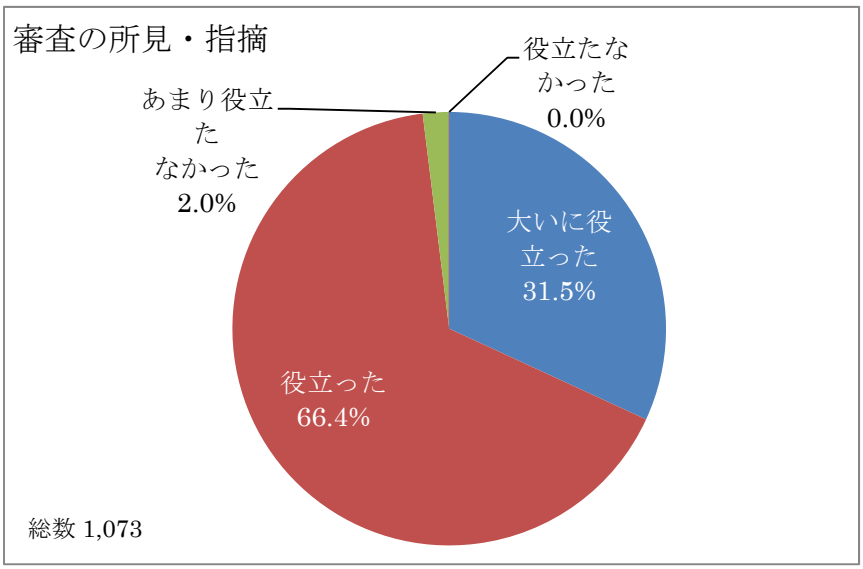


図 13-3　審査の所見・指摘

「あまり役立たなかった」点として指摘されたものの例は、次のとおり。

・記述レベルの指摘が多く、現実的な有効性のある指摘がなかった。
・もっと厳しくてもよかったかもしれない。
・指摘事項を改善しても、効率が向上するとは思えない。
・当社の業務内容や業務形態に踏み込んだ有用な改善コメントが少ない。
・実態に即した観察事項になっていない。
・指摘が細かいため、改善しても効果が薄い。

(4)審査の質に対する総合評価

審査の質に対する総合評価として、「満足」「やや満足」「やや不満」「不満」の４段階で評価していただいた。

評価は、「満足」(69.3%)、「やや満足」(28.9%)、「やや不満」(1.8%)、「不満」(0.0%)の順であった（図 13-4)。

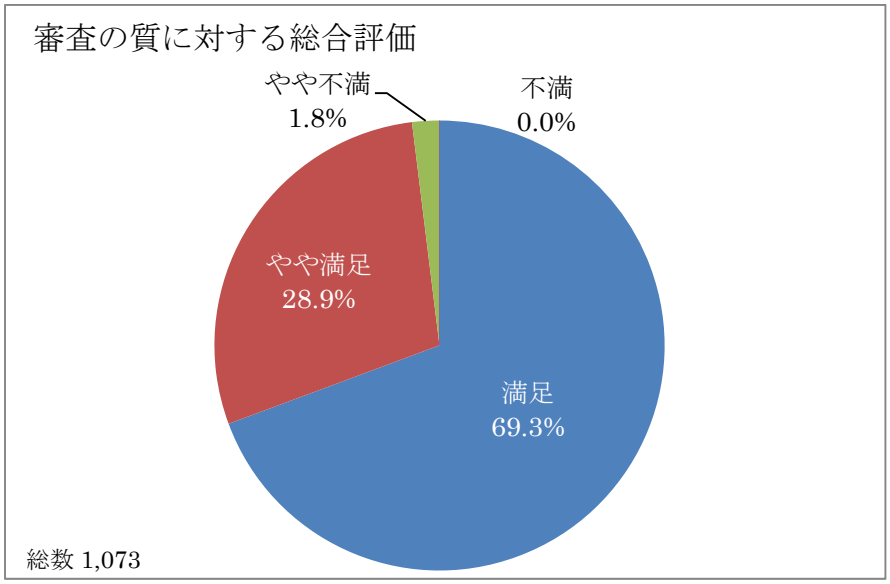


図 13-4　審査の質に対する総合評価

「やや不満」な点として指摘されたものの例は、次のとおり。

・審査員個人のコミュニケーション能力に難あり。
・もう少し細かく（すべてにおいて）指摘してもらってもよかった。
・自社サービスは多様化しているので、もう少しカスタマイズされた審査を期待したい。
・審査員が業務を理解していなかったと思われる点があった。
・プロセスの質を高められるような指摘が欲しい。
・QMS、ISMS 同時に審査を実施しているが、QMS に掛ける時間が多い。
・審査時間が長すぎる。
・審査員の力量に差がある。些細な事で指摘を受ける。
・自己流の解釈を押し付けるきらいがある
・審査員によりバラツキがある

質問１３と質問５とのクロス集計

審査の質に関する５つの項目の評価結果のうち、各項目の選択肢の「1」(「満足」、「適切」又は「大いに役立った」)を選んだ比率を、ISMS 認証取得後の経過年数の４階級ごとにクロス集計した結果を、図 13-5 に示す。

項目によって若干の差異があるものの、「質問１２と質問５とのクロス集計」の場合と概ね同様、ISMS 認証取得３年の再認証審査時期を境として、評価が段階的に下がる傾向がみられる

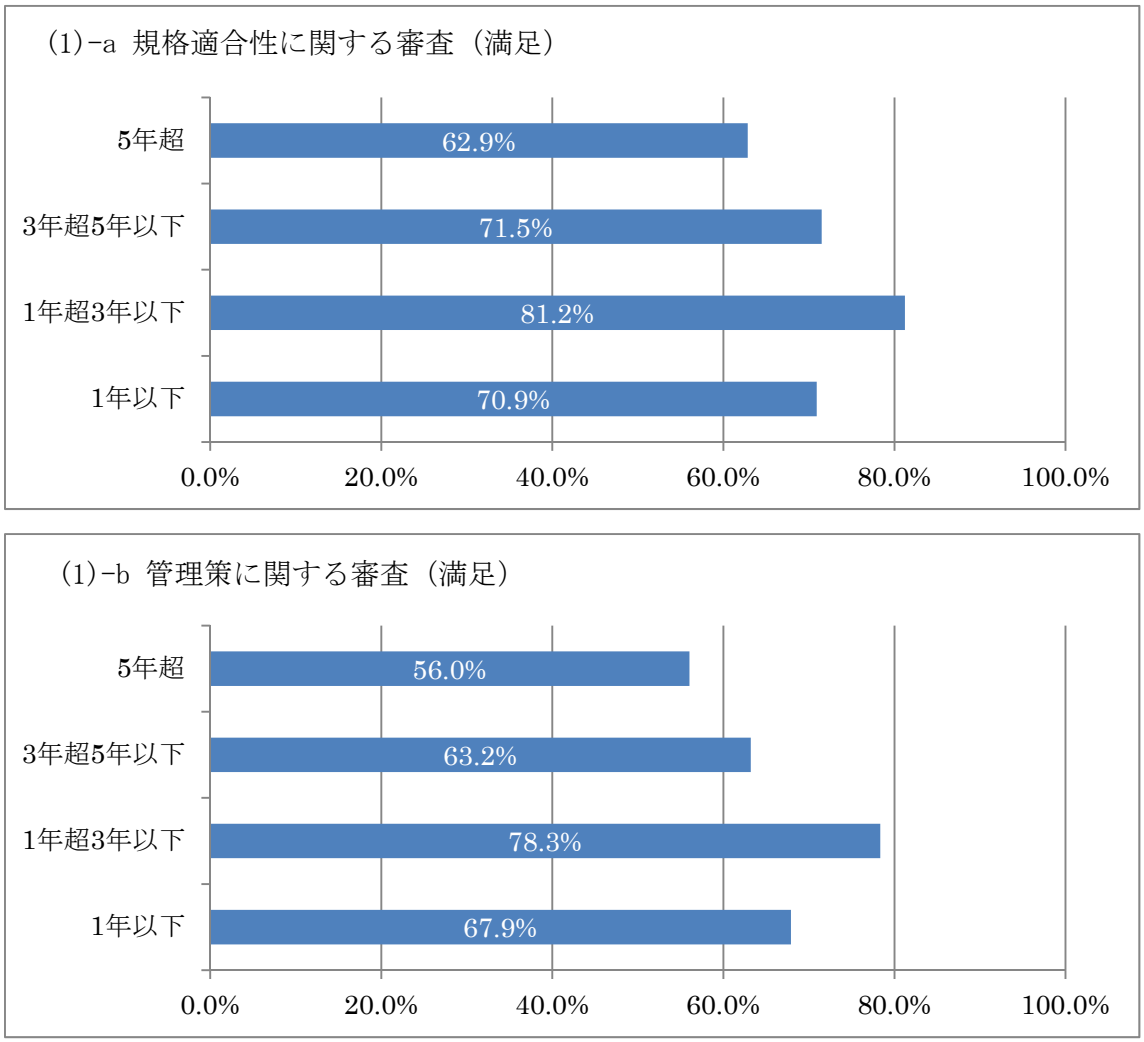
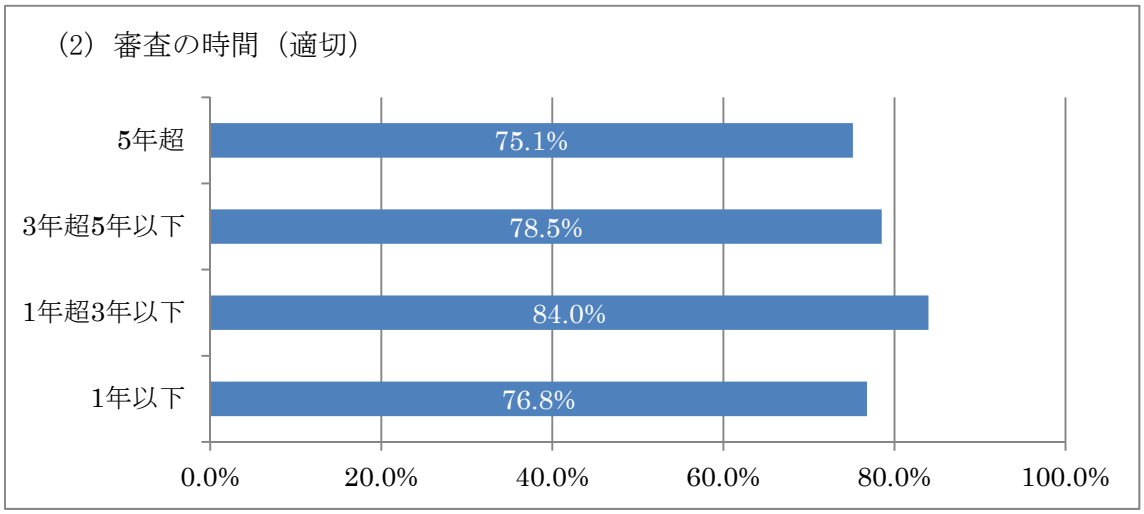
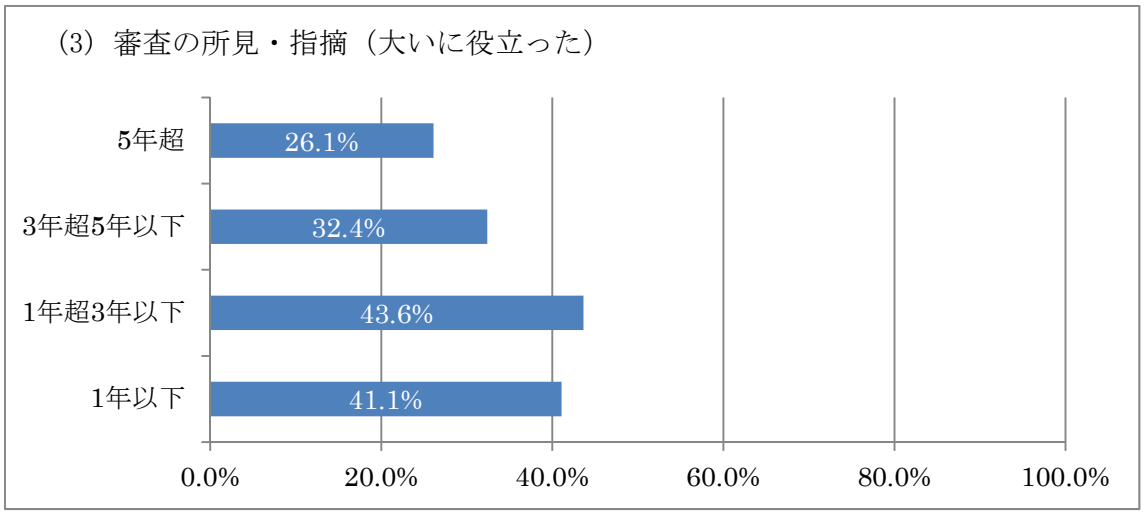


図 13-5　　経過年数区分と審査の質(1/2)





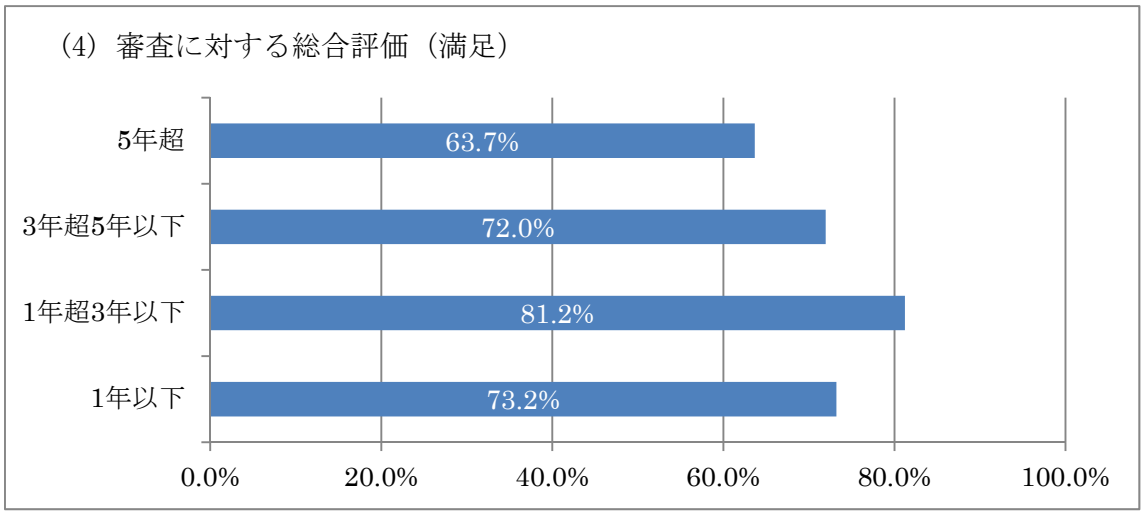


図 13-5　経過年数区分と審査の質（2/2）

質問　１４　認証審査及び審査員に対するご意見・ご要望

認証審査及び審査員に対するご意見・ご要望の内容を分類した結果は、図 14 のとおりである。

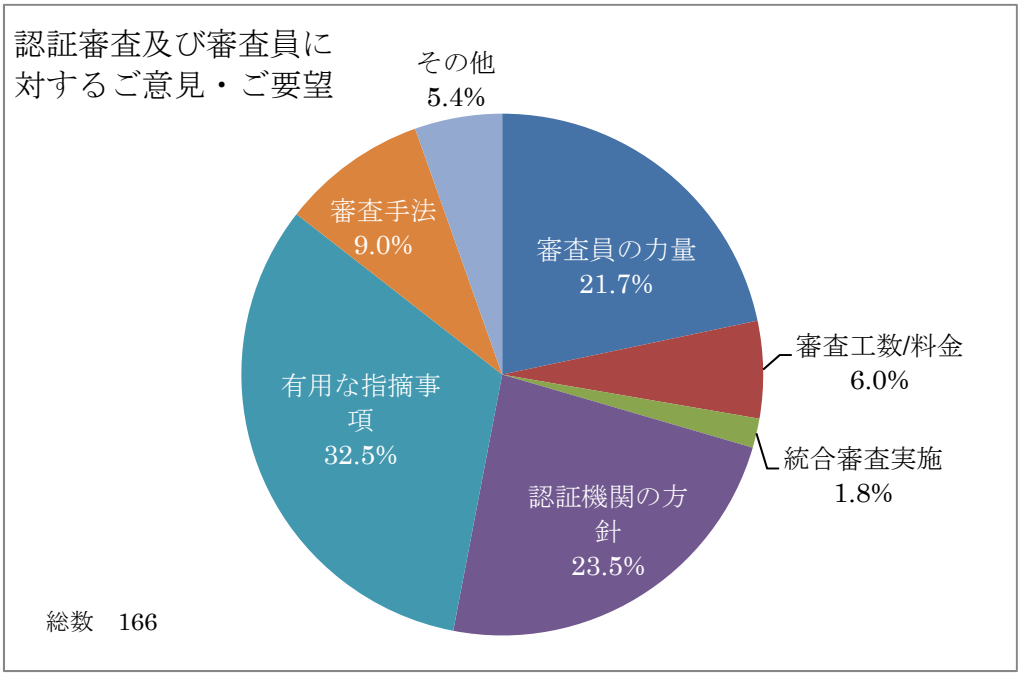


図 14　認証審査及び審査員に対するご意見・ご要望

分類項目ごとの回答内容の傾向について分析した結果は、次のとおり。

- 有用な指摘事項報告/助言

この分類項目に該当する意見、要望の多くは、審査において、受審組織にとってより有益な指摘、情報提供を求めるものであり、今後の改善活動に活かそうとする内容である。回答例を以下に記す。

・一般的な最新事情・成約等と当社固有の事情の双方をふまえた上で、適切かつ改善に有効な指摘
・事業所独特の問題等に対する積極的なアドバイス
・受審組織のマネジメントシステム改善につながる他社事例の紹介
・組織のマネジメント運用実態に対する 外部視点による弱点についての指摘
・同業(同規模)他社と比較した、受審組織のセキュリティレベルの提示

- 審査員の力量

この分類項目に該当する意見、要望の多くは、審査において、審査員の力量のバラツキや審査員によって見解が違う指摘事項により、対応することに対して戸惑うことがあるため、均一でかつ有益な情報の提供を求めるものであり、回答例を以下に記す。

・もう少し事前に、業務の理解ができると良い。

・レベルの均質化を望む。
・過去に審査員の主観での指摘があった。2 度とないようにしていただきたい。
・当社の組織や業務に則した審査を行ってほしい。

- 審査手法

この分類項目は、審査員個人の方針に関わると思われる審査の手法に関するものである。回答例を以下に示す。
・認証審査員にて、基準判断、考えが異なるため、審査員が変わる毎に基準があいまいになる。
・管理策の有効性を現場で見て欲しい
・審査を厳しくして欲しい。
・審査スケジュール調整を早めに、フレキシブルにして欲しい。
・考えが柔軟な比較的若い審査員を希望する。

- 認証機関の方針

この分類項目は、認証機関の方針によると思われるもので、回答例を以下に示す。
・同じ審査員による継続的な審査を希望
・外部へ公開可能な報告書の作成

- 審査工数/料金

ほとんどが審査時間の短縮、審査費用の低減に関する要望であったが、審査の間隔を長くしてほしいとの要望も若干あった。

- 統合審査の実施

この分類項目は、認証機関による複数のマネジメントシステムの同時審査を求めるものであり、回答例を以下に示す。
・QMS、EMS 等との複数認証における統合審査の実施
・プライバシーマーク審査との同時審査の実施

- その他

満足している旨の回答や、アンケート調査に関する回答、意図が把握できなかった回答などがここに含まれる。

認証機関の認定の信頼性について

質問１５　認定機関から認定を受けた認証機関の信頼性

認定機関から認定を受けた認証機関の信頼性について、認定の有無、国内の認定機関、MLA の効果、MS 認証懇親会の認知度の４つの観点で評価していただいた。

（１）　認定の有無

信頼性の材料判断の一つとして、認定の有無を 4 段階で評価していただいた結果、「重視した」（44.2%）、「やや重視した」（20.8%）、「多少は考慮した」（22.0%）、「まったく考慮しなかった」（13.0%）の順となった（図 15-1）。

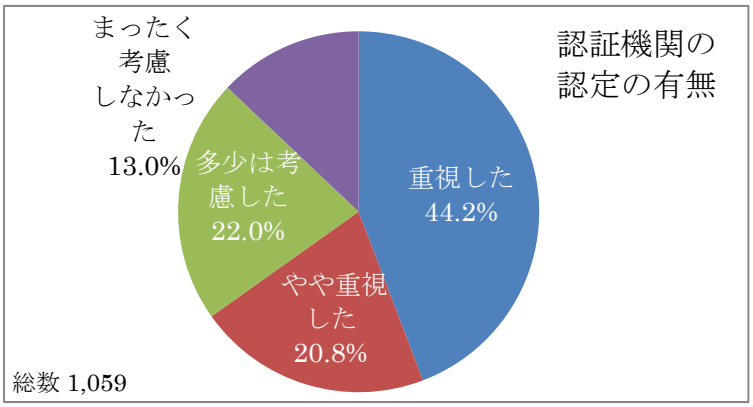


図 15-1　認定の有無を考慮

（２）　国内認定機関による認定

認証機関が国内の認定機関から認定を受けていることに関する意識を 4 段階で評価していただいた結果、「重視した」（38.9%）、「多少は考慮した」（24.3%）、やや重視した」（20.8%）「まったく考慮しなかった」（16.0%）の順となった（図 15-2）。

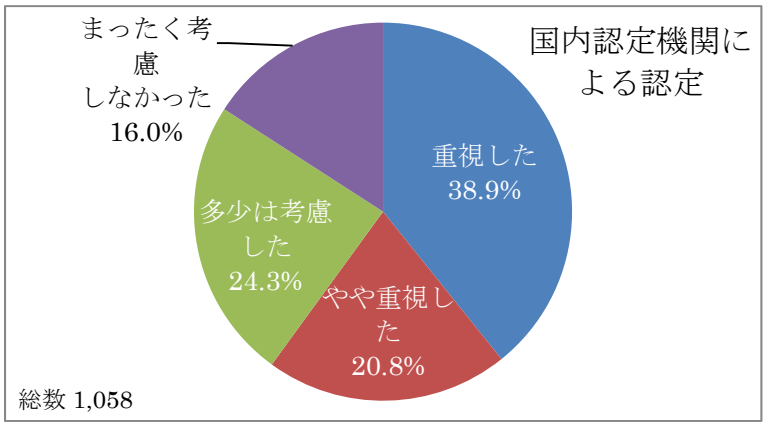


図 15-2　国内の認定機関からの認定

制度全般に対するご意見等

質問１６　海外のパートナーとの制度の活用

事業活動を海外展開している組織に対して、海外のパートナーとの制度の活用状況に関する調査結果を記す。

(1) 海外のパートナーから ISMS 認証の取得を確認されたり、ISMS 認証を取得していることをプラスに評価されたことがありますかとの質問に対して、回答は、「3 確認されたことはない」(75.6%)、「1 確認され、プラス評価されたことがある」(10.5%)、「2 確認されたことがあるが、プラス評価されたことはない」(14.0%)の順となった（図 16-1)。

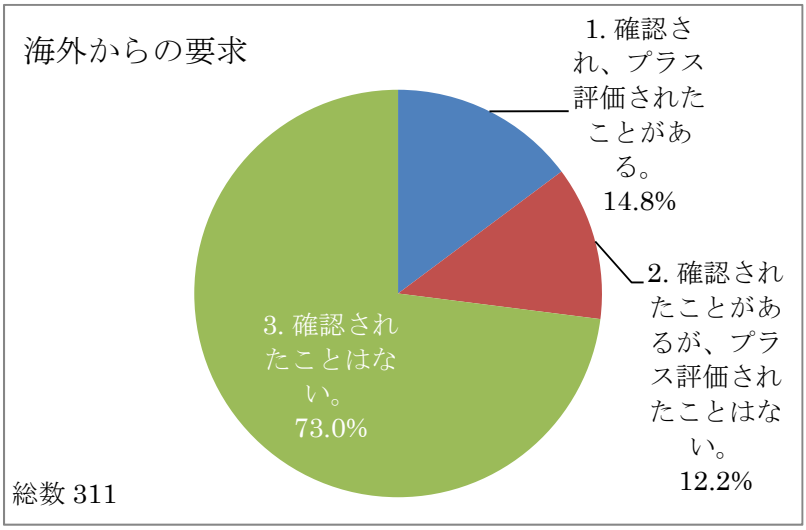


図 16-1　海外のパートナーとの制度の活用（海外からの要求）

(2) 海外のパートナーに ISMS 認証の取得を要求したり、海外のパートナーが ISMS 認証を取得する必要性を感じたりしていますかとの質問に対して、回答は、「1 要求している」(53.7%)、「2. 要求していないが、必要性を感じている」(41.8%)の順となった（図 16-2)。

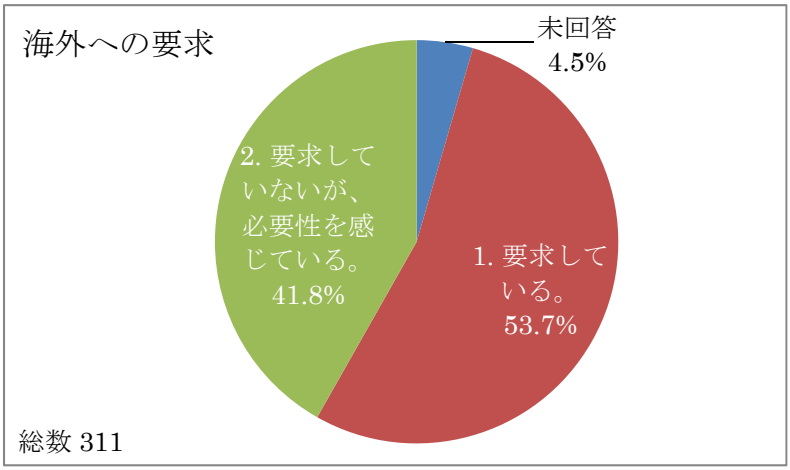


図 16-2　海外のパートナーとの制度の活用（海外への要求）

質問１７　本センターへの期待

複数回答のため、全項目の回答件数は 2,167 件である

回答内容を分類した結果は、図 17 のとおりである。

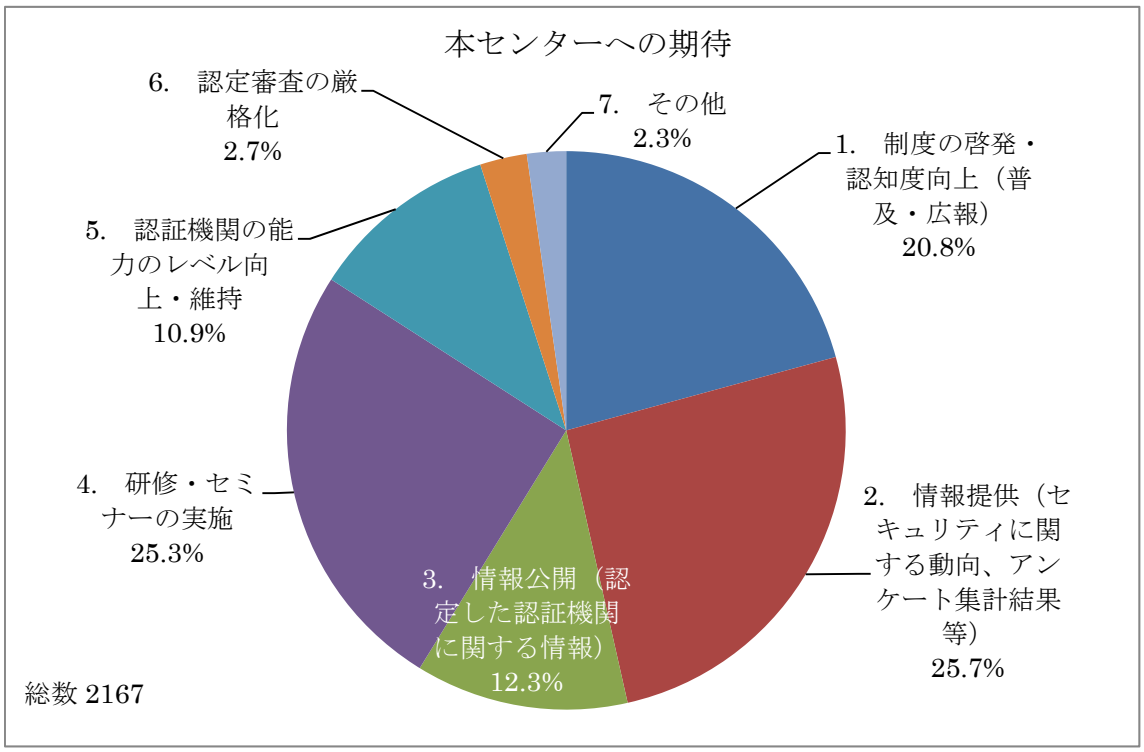


図 17　本センターへの期待

分類項目ごとの回答内容の傾向について分析した結果は、次のとおり。

[制度の認知度改善、制度推進]

この分類項目は、制度の広報、普及、運営推進、制度の活用に関するものである。回答例を以下に示す。

・世間での認知度が低いように感じます。一般人(IT 業界以外の方)への認知向上を期待します。

・特定の地域では特に ISMS の認識が低く、せっかく取得し維持しても組織の体制は整ってもあまり広報という面では活かされていない。もっと ISMS を普及させてほしい。

・ISMS は管理策があるから有効な認証制度の様に思います。2013 年度版では ISO31000 等の影響を大きく受けたと伺っていますが、形骸化されないことを望みます。

[情報提供]

この分類項目は、制度の認知度改善、制度推進の手段としての情報公開に関するものである。回答例を以下に示す。

・ホームページ等でクラウド、電子メール、物理媒体など多種多様な情報資産に対するリスクアセスメント(脅威・脆弱や対応策）の例を示していただけると情報セキュリティの強化の参考になります。
・業種による特性を考えた指示、指導がいただけるとありがたいです。
・有効な活動の照会など。
・セキュリティに対する取り組みの最新事例等の公開をお願いします。

[研修、セミナー]

この分類項目は、研修、セミナーの実施に関するものである。要望のあったテーマの例を以下に示す。
・地方開催のセミナー等、御検討をお願い致します。
・内部監査員や管理責任者、スキルアップのための定期教育を e-learning 等で検討いただきたい。

[審査員、認証機関]

この分類項目は、審査員の力量、認証機関の能力、方針、営業活動に関するものである。
回答例を以下に示す。
・審査員の更なるレベル向上(インシデント予防に実効あるコメントを期待するとともに審査員のレベルのバラツキを極力なくす)。
・認証機関の審査レベルの差をなくす取り組みに期待する。
・不適合を出さなくなった審査員が非常に多くなった。本質にかかわらないことを指摘し、お茶を濁しているように感じる。
・認証機関の能力レベルの公開。

[審査工数、費用]

この分類項目では、審査費用、登録・維持費用の低減に関する要望が多かった。
回答例を以下に示す。
・取得費用が掛かりすぎる
・企業規模や審査内容により料金体系を考えてほしい

[認定審査]

この分類項目での回答例を以下に示す。
・国内の認定機関と海外の認定機関の差異の明確化。メリット、デメリットまで。
・「当社に切り替えれば楽になります。」というような営業をかけてくる大手認証機関が実際にありました。このような情報も吸い上げたほうが良いと思います。

・認証機関や審査員間でレベル差(力量、規格解釈等)がなくなるよう取り組みを行っていただきたい。

[ガイドライン、規格]

この分類項目は、規格、基準の制定、改訂に関するものである。

・ISMS の実務に役立つツール、テンプレート、解説文書の公開を期待します。

・ISO27001:2013 の新規格に則したガイドラインや解説書の作成を期待します。

[プライバシーマーク制度関連]

この分類項目での回答例を以下に示す。

・プライバシーマーク制度との統合（重複した MS が多く企業の負担になっているため）

・プライバシーマークと ISO27001 が 1 つの規格になると非常に運用がしやすい。

・ISMS とプライバシーマークの審査を同一審査機関で行えるようにして欲しい。別々であるがために二度手間を感じ社内運用も効率が良くない

[その他]

この分類項目での回答例を以下に示す。

・認証登録を公開していることで、関連するサービス事業者からの営業の電話、ＤＭのターゲットになっている。

質問１８　制度全般に対するご意見・ご要望

制度全般に対するご意見・ご要望を分類した結果は、図 18 のとおりである。

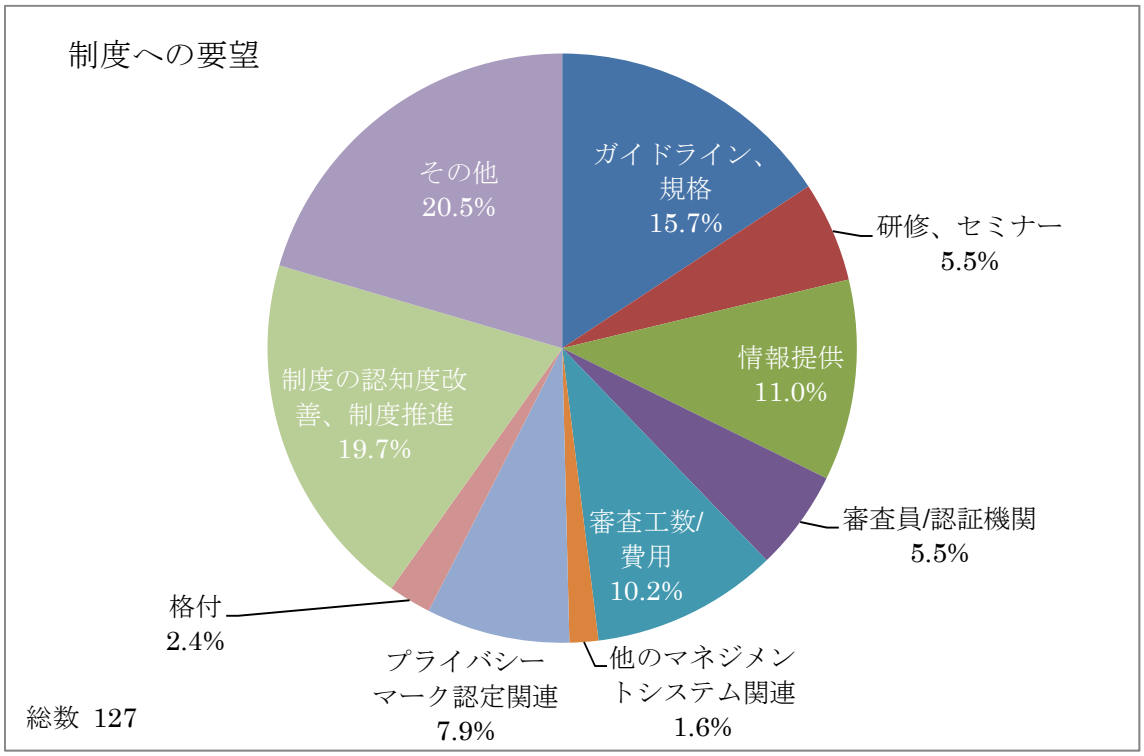


図 18　制度全般に対するご意見・ご要望

分類項目ごとの回答内容の傾向について分析した結果を述べる。

[制度の認知度改善、制度推進]

ISMS 制度の認知度向上の要望が、当該分類項目全体の 19.7%となっている。

内容として次のようなものがある。

・ISMS の認知度(メリット含め)をさらに向上してほしい

・ISMS は敷居が高いイメージを持たれているが、そのあたりの払拭をお願いしたい。

[情報提供]

ISMS に関する有益な情報を、他社事例や最新の規格の動向などを含めて情報公開する要望が多かった。

またこれらの中には、急速に変化している情報セキュリティをめぐる環境に対応できるよう、有効な仕組みや考え方などの要望も含まれている。

[研修、セミナー]
回答例を以下に示す。
・今後の規格改定情報等を含め、情報提供やセミナーの開催を望む。
・ISO/IEC 27001:2013 への移行審査受審に備えるアドバイスがあれば、有り難い。
・ISMS 規格改訂については認証機関のセミナーとは別に、認定機関として説明会等を開催し、説明をする必要がある。
・適合性評価制度の無料セミナーを各地方で実施していただきたい。

[認証機関、審査員]
回答例を以下に示す。
・審査を厳しくして認証維持のメリットをもっとアピールして欲しい。
・問題点の指摘だけでなく、助言もしっかりして頂きたい

[認証審査工数、費用]
審査費用、登録・維持費用の低減に関する要望が多かった。

[ガイドライン、規格]
回答内容は、規格の日本語が分かりにくいという意見が多く、この分類項目の大半を占めた。他に、規格の要求事項の中に、スマホ、タブレットをはじめとしたモバイルデバイス、あるいはクラウドの標準化等、規格が要求する事項との紐付解釈が難しく、指針をわかりやすく設けてほしいなどの内容の要望があった。

[プライバシーマーク制度との関連]
ISMS 制度とプライバシーマーク制度との調和、統合を求める意見があった。

[格付]
同じ「適合」でも、レベルが高いのか、低いのかが判るような、「格付化」を検討頂きたい。自分たちのレベルが判ると同時に、ビジネスパートナーのレベルを確認できるのは有意義といった意見があった。

[その他]
満足している旨の回答、意味不明の回答などのほかに、今回のアンケート調査に関する意見、要望が数件あった。

おわりに

ISMS 制度のユーザーである組織と本協会とが直接情報交換する機会は、制度の説明会、セミナーなどの制度の普及、広報活動の場や、Web による情報提供、Q&A に限られていましたが、今回、アンケート調査により、数多くの組織から生の声を聞くことができ、大変有意義な結果を得られました。

ISMS 制度は、QMS、EMS などに比べると歴史が浅く、認証を取得して間もない組織が多い。組織のマネジメントシステムと同様、制度自体も発展途上にあります。このことがアンケート調査結果に反映されており、組織のマネジメントシステムを改善するための具体策に尽力されていることがうかがえ、これが審査や制度推進に対する具体的な要望となって表現されています。

また、マネジメントシステムを構成する人的側面の重要性を認識されており、これが人材育成、教育を今後の主な課題としている組織が多いことで示されています。

一方、技術的な側面に関しての具体的な課題も多く、組織にとって役に立つ情報を提供することが求められています。

ISMS は、将来起こり得るリスクに備えるための仕組みであり、日常の事業活動のアウトプットに必ずしも直結しないため、費用対効果を説明しにくいという特質がありますが、これが、経営者の ISMS に対する投資を消極的にさせる要因の一つになっているものと思われ、今回の調査でも、審査、登録、維持に対する費用の低減を求める意見が多く見られました。

ISMS 制度を運用する側の認定機関、認証機関の役割は、審査の信頼性を高め、組織の ISMS の価値を高めることにあります。このためにも、今回のアンケート調査結果を最大限に活用させていただく所存です。

本報告書は、本制度に関する様々な立場の関係者に読んでいただき、各々の立場で課題の解決に尽力されることを願いまして結びとします。

付録　ISMS 適合性評価制度に関するアンケート調査書

平成 25 年度

ISMS 適合性評価制度に関するアンケート調査書

2014 年 2 月 25 日

一般財団法人 日本情報経済社会推進協会(JIPDEC)
情報マネジメント推進センター

平成 25 年度

ISMS 適合性評価制度に関するアンケート調査書

はじめに

ISMS 適合性評価制度は、民間主体の制度として 2001 年度にスタートし、約 1 年間のパイロット運用を経て、2002 年 4 月から本格運用に入り、今日に至っております。

この間、コンピュータ処理への依存度の高まりやインターネットの爆発的な広がりとともに、それに比例して情報資産への脅威も増大し、システムや人的な脆弱性を突いたセキュリティ事故も件数、規模ともに増加してきています。このような背景から、自社のみならず取引先における情報セキュリティのリスクをマネジメントする重要性についての認識は格段に高まってまいりました。

これを受けて 2008 年及び 2011 年に、ISMS 制度の実態を把握し、制度の信頼性をより高めることを目的としてアンケートを実施しました。本調査は、前回調査から 2 年が経過し、新たに約 500 の組織が認証を取得されたことから、現時点での ISMS 適合性評価制度の状況を確認するとともに、ISMS 導入及び認証の有効性を検証し、制度の改善を図ることを目的としています。

アンケート調査にお答えいただく前に

アンケート調査に回答いただく前に、下記の回答情報の取扱方針に対して、記入者の同意をいただくことにしております。同意いただける場合は、下記のチェック個所に記入いただいた上、本ページを含めてご返送ください。

本アンケート調査では回答者の所属、氏名、連絡先等の情報を記入いただくことにしております。これらの個人情報を含む回答情報は、一般財団法人日本情報経済社会推進協会(JIPDEC)の個人情報保護方針*に基づいた下記の方針にしたがって利用させていただきます。

注*　http://www.jipdec.or.jp/ov/kojin.html

［個人情報管理者］

本アンケート調査業務における個人情報管理者は下記のとおりです。

一般財団法人日本情報経済社会推進協会(JIPDEC) 専務理事

［個人情報の取扱いについて］

当センターでは、回答欄に記入いただいた個人情報を、本アンケート調査内容に関する確認及びアンケート調査結果のご報告のために使用いたします。当センターは、これらの業務を含むアンケート調査に関わる業務の一部を外部委託いたします。外部委託事業者は、十分な保護水準を満たしており、契約等により適切な処置を講じています。

当センターが取得した個人情報は、上記によるものの他、法令等による場合を除いて第三者に提供することはありません。

当センターが取得した個人情報の安全管理のために、必要かつ適切な措置を講じます。
当センターが取得した個人情報は、本人からの開示、訂正、削除、利用停止等の要請に対して遅滞なく対応いたします。
［回答内容全体について］
回答情報は、ISMS 適合性評価制度全般の運用状況を把握し、今後同制度を改善するために使用します。貴組織名を特定した回答情報は公開いたしません。
［集計・分析結果について］
回答情報を集計・分析した結果は報告書にまとめ、当センターの HP で公開いたします。

上記の方針に同意いただけるでしょうか。**□内にチェック印を記入してください。** □同意する □同意しない

同意いただける場合、以下のアンケート調査にご協力ください。

記入要領

質問項目は全部で、18 問です。回答は、該当する番号に○印を付けていただくものと、回答情報を記入していただくものとがあります。

調査書の返送について

調査書は、同封の返信用封筒に入れて、郵送してください。
回答期日：２０１４年３月５日（水）までにご回答をお願いいたします。

連絡先

一般財団法人日本情報経済社会推進協会(JIPDEC)　情報マネジメント推進センター
電話番号：03(5860)7570
FAX 番号：03(5573)0564

※本アンケート実施に関しては、http://www.isms.jipdec.or.jp/enquete/2014/　もご覧ください。(本アンケート用紙の word 版入手方法のご案内もございます)

基本情報について

貴法人名及び回答者の所属、氏名、連絡先等について記入してください。

法人名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

回答者

所在地：〒＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

所属、役職：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

氏名：＿＿＿＿＿＿＿＿＿＿＿＿

連絡先：E-Mail＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

TEL＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

質問１　貴法人の業種を、下記の業種区分から選択してください。複数業種に関連する場合は、主力業種１つのみ選択してください。12、21 又は 23 を選択した場合、(　)の中に業種を記入してください。18 を選択した場合、さらに 18-1 から 18-11 から該当するものを１つのみ選択してください。18-11 を選択した場合、(　)の中に業種を記入してください。

1. 食料品･飲料･タバコ等の製造業
2. 衣服･天然素材繊維製品の製造業
3. 木材･木製品･パルプ･紙等の製造業
4. 出版･印刷業
5. 化学薬品･化学製品(化学繊維を含む)･医薬品の製造業
6. 石油･石炭･ゴム･プラスチック等の製造業
7. ガラス･セラミック･コンクリートの製造業
8. 鉄鋼･非鉄金属業･金属製品の製造業
9. 機械･機器の製造業
10. 電気/電子機器･光学的装置製造業
11. 輸送機器製造業
12. その他の製造業（＿＿＿＿＿＿＿＿）
13. 建設業(エンジニアリングを含む)
14. 廃棄物処理業･再生業
15. 電力･ガス･熱･水道供給業
16. 卸売･小売業
17. 金融･保険･不動産業
18. 情報技術
    - 18-1　通信業
    - 18-2　放送業

18-3　システムインテグレーション業
18-4　受注ソフトウェア業
18-5　ソフトウェアプロダクト業
18-6　計算事務等情報処理業
18-7　システム等管理運営受託業
18-8　データベースサービス業
18-9　インターネット附随サービス業
18-10　映像・音声・文字情報制作業
18-11　その他（＿＿＿＿＿＿＿＿＿＿）
19. ホテル･レストラン業
20. 医療関係
21. その他サービス業（＿＿＿＿＿＿＿＿＿＿）
22. 公共･行政･教育機関
23. 分類不明（＿＿＿＿＿＿＿＿＿＿）

質問２　貴法人が株式会社の場合、貴法人の資本金について、下記のうち該当するものを選択してください。
1. 5000 万円以下
2. 5000 万円超、1 億円以下
3. 1 億円超、3 億円以下
4. 3 億円超

質問３　貴法人が常時使用する従業員（全社）の数について、下記のうち該当するものを選択してください。
1. 5 人以下
2. 5 人超、20 人以下
3. 20 人超、50 人以下
4. 50 人超、100 人以下
5. 100 人超、300 人以下
6. 300 人超

質問４　ISMS 取得の認証範囲についてお答えください。
(1)　貴組織における認証範囲（一部認証の場合は従業員数の割合）をお答えください。
1. 全社　　2. 全社の 75%以上　　3. 全社の 25%～75%　　4. 全社の 25%未満
(2)　認証範囲の従業員数を概数でお答えください。
約（＿＿＿）人

(3) 認証範囲に特筆すべき特徴（例えば「グループ企業による取得」、「海外サイトを含む」等）があれば記入してください。

ISMS 認証の実績等について

質問５ 貴組織が ISMS 認証を初めて取得してから現在までの経過年数及び現在の認証登録番号をお答えください。

経過年数（　　年　　か月）　　認証登録番号（　　）

質問６ 貴組織では、ISMS 以外にどのようなマネジメントシステム認証を取得していますか。複数所得されている場合は、その全てに○を付けてください。

1. ISO 9001(品質)
2. ISO 14001(環境)
3. ISO/IEC 20000(IT サービス)
4. ISO 22301(事業継続)
5. その他（　　）

質問７ 貴組織が ISMS 認証を初めて取得してから現在までの間に認証機関(審査機関)を変更した、または変更することを検討されたことがあるかお答えください。

1. 変更を考えたことはない
2. 変更を考えたが、実行していない
3. 1 回変更した
4. 2 回以上変更した

上記で 2～4（認証機関の変更を考えたことがある、あるいは実際に変更した）を選択された方は、その理由として最も当てはまるものをお答えください。

1. 審査内容（深さや指摘内容等）が不満
2. 認証機関のサービス（情報提供等）や対応（手続き等）に不満
3. 審査料金の比較
4. その他（　　）

ISMS の導入及び認証取得の効果等について

質問８　ISMS 導入の目的又は動機について、下記の各項目が該当するか否かをお答えください。

No.	項　　目	該当する	やや該当する	余り該当しない	該当しない
1	組織の情報セキュリティ管理体制の強化のため	1	2	3	4
2	組織の情報セキュリティ対策の強化のため	1	2	3	4
3	社員の情報セキュリティに関する意識向上、教育啓発のため	1	2	3	4
4	入札、受注の条件、取引先からの要請による	1	2	3	4
5	顧客からの信頼を確保するため	1	2	3	4
6	企業イメージの向上のため	1	2	3	4
7	同業他社との差別化、営業上の優位性の確保のため	1	2	3	4
8	全社の方針による	1	2	3	4
9	インシデント発生を抑制するため	1	2	3	4

上記 1～９以外に、目的又は動機として意識された事項がありましたら、記入してください。

質問９　ISMS を導入し、認証を取得された効果について、下記の各項目が該当するか否かをお答えください。

No.	項　　目	該当する	やや該当する	余り該当しない	該当しない
1	組織の情報セキュリティ管理体制が強化できた	1	2	3	4
2	組織の情報セキュリティ対策が強化できた	1	2	3	4
3	社員の情報セキュリティに関する意識向上、教育啓発に寄与した	1	2	3	4
4	顧客からの信頼確保に貢献した	1	2	3	4
5	企業イメージの向上に貢献した	1	2	3	4
6	営業上、同業他社に対する優位性の確保に貢献した	1	2	3	4
7	事業の収益向上に貢献した	1	2	3	4
8	IT 統制、J-SOX 法対応に有効であった	1	2	3	4
9	情報面での事業継続性の向上に有効であった	1	2	3	4

10	法遵守（コンプライアンス）の面で有効であった	1	2	3	4
11	ソフトウェアの資産管理に有効であった	1	2	3	4
12	情報セキュリティインシデント発生の抑制に効果があった	1	2	3	4
13	リスク評価の方法が定着した	1	2	3	4
14	組織の情報セキュリティレベルが期待値に達した	1	2	3	4
15	組織の情報セキュリティは期待するレベルを維持している	1	2	3	4
16	経営者の情報セキュリティに対する関与が深まった	1	2	3	4

上記項目№1～16 で 1(該当する)を選択された場合、また№1～16 以外に効果として特筆すべき事項がありましたら、その具体的な内容や例を差し支えない範囲で記入してください。

質問１０　顧客から、貴組織の情報管理リスクの把握のため、例えば実査、監査報告書の開示など、ISMS 認証文書（登録証）の他に求められたことがありますか。あればどのようなものでしたか、差し支えない範囲で記載してください。

1. 求められたことがある（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
2. 求められたことはない

質問１１　貴組織の ISMS 認証取得、維持に関する今後の主な課題について、差し支えない範囲で記入してください。

審査員の力量及び審査の質について

質問１２　最近受審された ISMS 認証審査において、審査員の力量を下記の観点で評価してください。

No.	項　　目	十分である	概ね十分である	やや不十分である	不十分である
1	マネジメントシステムに関する知識及び業務経験	1	2	3	4
2	情報システム、情報セキュリティに関する知識及び業務経験	1	2	3	4
3	受審組織の業務に対する理解	1	2	3	4
4	コミュニケーション能力	1	2	3	4
5	審査技術	1	2	3	4
6	改善課題を指摘する能力	1	2	3	4

質問１３　最近受審された ISMS 認証審査の質を下記の観点で評価してください。

［審査の内容］

(1)-a　マネジメントプロセス、マネジメント文書の規格適合性に関する審査内容を、下記の４段階で評価してください。３又は４を選択された場合は、不満な点を簡潔に記入してください。

1. 満足
2. やや満足
3. やや不満（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
4. 不満（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

(1)-b　管理策に関する審査内容を、下記の４段階で評価してください。３又は４を選択された場合は、不満な点を簡潔に記入してください。

1. 満足
2. やや満足
3. やや不満（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
4. 不満（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

［審査の時間］

(2)　組織の ISMS の有効性を含む実施状況の評価に関する審査時間を、審査の信頼性の観点から、下記の項目で評価してください。

1. 適切
2. 長い
3. 短い
4. 何とも言えない

［審査の所見・指摘］

(3)　審査所見・指摘の、マネジメントプロセス、マネジメント文書、管理策、及びそれらの運用を改善するうえでの有効性を、下記の４段階で評価してください。３又は４を選択された場合は、役立たなかった点を簡潔に記入してください。

1. 大いに役立った
2. 役立った
3. あまり役立たなかった（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
4. 役立たなかった（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

［審査に対する総合評価］

(4)　総合的に見た審査の質を、下記の４段階で総合評価してください。３又は４を選択された場合は、不満な点を簡潔に記入してください。

1. 満足
2. やや満足
3. やや不満（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
4. 不満（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

質問１４　今後の認証審査及び審査員に対して、ご意見、ご要望等がございましたら、記入してください。

認証機関の認定の信頼性について

質問１５　認定機関から認定を受けた認証機関による ISMS 認証の信頼性について、最も当てはまると思うものをご回答ください。また(1)～(2)については、その理由を簡潔に記入してください。

(1)　認証機関の信頼性の判断材料の一つとして、認定の有無を考慮しましたか。

1. 重視した　2. やや重視した　　3. 多少は考慮した　　4. まったく考慮しなかった

(理由)

(2)　認証機関が、国内の認定機関から認定を受けていることを意識しましたか。

1. 重視した　2. やや重視した　　3. 多少は考慮した　　4. まったく考慮しなかった

(理由)

制度全般に対するご意見等

質問１６　貴組織が事業活動を海外展開されている場合のみ、ご回答ください。

(1)　海外のパートナーから ISMS 認証の取得を確認されたこと、あるいは貴組織が ISMS 認証を取得していることをプラスに評価されたことがありますか。

1. 確認され、プラス評価されたことがある。
2. 確認されたことがあるが、プラス評価されたことはない。
3. 確認されたことはない。

(2)　海外のパートナーに ISMS 認証の取得を要求したり、海外のパートナーが ISMS 認証を取得する必要性を感じたりしていますか。

1. 要求している。
2. 要求していないが、必要性を感じている。
3. 要求していないし、必要性も感じていない。

質問１７　認定機関として、認証機関を認定する立場にある当センターに期待することがございましたら、該当する項目に○（複数可）をするか、その他の欄に記入してください。

1. 制度の啓発・認知度向上（普及・広報）
2. 情報提供（セキュリティに関する動向、アンケート集計結果等）
3. 情報公開（認定した認証機関に関する情報）
4. 研修・セミナーの実施
5. 認証機関の能力のレベル向上・維持
6. 認定審査の厳格化
7. その他

質問１８　ISMS 適合性評価制度全般に対して、ご意見、ご要望等がございましたら、記入してください。

以上

アンケートにご協力いただき、ありがとうございました。

※回答を返送いただく前に、２ページにある個人情報の取り扱いに関する同意欄にチェックがあることをご確認下さい。